UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

CONFLICT ARMAMENT RESEARCH

PERMANENT MISSION OF THE UNITED ARAB EMIRATES TO THE UNITED NATIONS NEW YORK

Autonomous and Remotely Operated Systems

AROS PROGRAMME

Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes

UNOCT AROS Programme and Conflict Armament Research

Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes

United Nations Office of Counter-Terrorism,

Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS Programme)

Conflict Armament Research

Contents

Boxes, tables and figures

Boxes

Tables

Figures

Foreword

The development of autonomous and remotely operated systems for economic purposes and everyday use has accelerated rapidly over the past decade. Unfortunately, so too have the ways non-State armed groups have adapted them for terrorist purposes, including the use of widely available and relatively low-cost unmanned aircraft systems (UAS) to conduct reconnaissance and attacks, record propaganda, and identify vulnerabilities and opportunities. To counter this threat, the international community must work together to prevent and counter the acquisition, weaponization and deployment of UAS technology for terrorist purposes.

During the eighth review of the United Nations Global Counter-Terrorism Strategy, in 2023, Member States expressed deep concern over the potential use of new and emerging technologies for terrorist purposes, such as the weaponization of commercial drones, and called upon all Member States to consider additional measures to counter the use of such technologies for terrorist purposes consistent with their obligations under international law, while strengthening international cooperation to prevent and combat terrorism.

To better understand Member States' needs and experiences and to guide international assistance efforts, the United Nations Office of Counter-Terrorism (UNOCT) and Conflict Armament Research (CAR) produced a first-of-its-kind baseline, the Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes. In 2022 and early 2023, UNOCT and CAR conducted interviews with Member States, United Nations entities, intergovernmental organizations, civil society and the private sector. They prepared, disseminated and analysed an information-gathering questionnaire to all Member States, and hosted a three-day global consultation with Member States. The outcome of those activities has enabled the Global Report to include the identification and exploration of commonalities and provide recommendations for Member States in efforts to prevent and mitigate threats and risks posed by the terrorist use of UAS.

I would like to express my sincere gratitude to CAR for its invaluable support and dedication to the development of this Global Report, and to all Member States, organizations and individual experts for sharing their insights and offering their time and expertise. I would also like to extend my utmost appreciation to the United Arab Emirates for the generous financial contribution, without which this critical global baseline would not have been possible. UNOCT remains committed to continuing such collaborative partnerships to further develop the Global Report as it intends to be a living document offering Member States valuable insights and informing counter-terrorism measures for years to come.

Vladimir Voronkov

Under-Secretary-General for
Counter-Terrorism

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

Executive summary

The use of unmanned aircraft systems (UAS) by non-State armed groups, including for terrorism-related purposes, is a grave and growing international security threat. From reconnaissance to preparing ambushes, dropping explosives on high-value targets, recording propaganda, "swarming" defence systems or crashing systems into vulnerable infrastructure, the use by non-State armed groups of UAS for terrorist purposes presents an acute security challenge for Member States. In response, Member States have increasingly focused on how to collectively prevent and address the use of UAS for terrorist purposes by non-State armed groups.

In 2022 and 2023, the United Nations Office of Counter-Terrorism, in association with Conflict Armament Research, undertook extensive consultations with Member States to conduct an initial exploratory study of how non-State armed groups are accessing and using UAS for terrorist purposes. That study served as the basis for this first global baseline of Member States' experience of the ways in which non-State armed groups seek to access and use UAS, including for terrorism-related purposes. The present report also seeks to provide insights into priority concerns for future developments. The research team intends to revisit and expand on the findings identified in this report in the future, to continue to monitor the evolving threat.

This report is divided into three main "pillars": acquisition, weaponization and deployment. The first pillar asks how non-State armed groups are seeking to procure or access UAS. It tests a nascent typology of acquisition approaches, identifying six primary pathways, including purchases of commercial systems, and illicit manufacture. It also focuses on knowledge transfer and the concern that cooperation between non-State armed groups will facilitate greater proliferation of UAS in the future.

The second pillar focuses on how non-State armed groups attempt to modify UAS in their possession, especially where the modifications may be part of efforts to "weaponize" UAS. It highlights in particular the growing concern that non-State armed groups are looking to further develop the knowledge, materials and tools to equip commercial UAS with the ability to drop explosive payloads or else act as a one-way attack (also referred to as single-use unmanned aerial vehicles). Notably, actual weaponization observation was not widely reported by Member States engaging in this research. However, several noted efforts towards this capability, and the concern that it may only be a matter of when, not if, this threat becomes a reality. The report also highlights the rapid development of artificial intelligence (AI) and the potential for this technology to be of significant concern if it was to be accessed and integrated into UAS by non-State armed groups, including for terrorism-related purposes.

The third pillar asks in what circumstances non-State armed groups look to deploy UAS. It identifies 12 deployment types, of which the most prominent is to conduct intelligence, surveillance and reconnaissance activities. Member States also focused on the disruption or observation of critical infrastructure as a key concern for non-State use of UAS.

The present report identifies four main trends:

1. Non-State armed groups are primarily exploiting commercial sources to access UAS.
2. While advanced military capabilities currently lie outside the reach of many non-State armed groups, there is evidence that some are seeking to establish local industrial capabilities to modify and enhance systems in their possession.
3. Non-State armed groups may be – and in some cases already are – sharing this knowledge with other organizations.
4. While unarmed UAS have to date been the predominate type used for terrorist purposes, there is a serious threat that future attacks will not only increase in frequency and geographic scope, but also increase in lethality, range, precision and power.

Consultations with Member States and other expert stakeholders highlighted a range of intervention points relevant to countering non-State use of UAS. The preventative and response measures highlighted in this report serve as examples of good practices that could be considered for implementation by Member States and other relevant stakeholders.

This report draws on, and seeks to build upon, existing frameworks, guidelines and research efforts in this area of work. It presents a list of identified good practices (a "threat reduction framework"), which could serve as a reference tool to help Member States and other relevant stakeholders to counter the non-State use of UAS across the pillars of acquisition, weaponization and deployment.

About the research partners

United Nations Office of Counter-Terrorism

The United Nations Office of Counter-Terrorism (UNOCT) was established on 15 June 2017 through the adoption of General Assembly resolution 71/291. The creation of the Office is considered as the first major institutional reform undertaken by the Secretary-General, António Guterres, following his report on the capability of the United Nations system to assist Member States in implementing the United Nations Global Counter-Terrorism Strategy (A/71/858). The United Nations Global Counter-Terrorism Strategy (General Assembly resolution 60/288) and its biennial General Assembly review resolutions provide the substance of the Office's mandate.

UNOCT has five main functions:

- Provide leadership on General Assembly counter-terrorism mandates entrusted to the Secretary-General from across the United Nations system
- Enhance coordination and coherence across the Global Counter-Terrorism Coordination Compact entities to ensure the balanced implementation of the four pillars of the United Nations Global Counter-Terrorism Strategy
- Strengthen the delivery of United Nations counter-terrorism capacity-building assistance to Member States
- Improve visibility, advocacy and resource mobilization for United Nations counter-terrorism efforts
- Ensure that due priority is given to counter-terrorism across the United Nations system and that the important work on preventing violent extremism is firmly rooted in the Strategy.

The General Assembly establishes the priorities of UNOCT through the resolutions of the biennial review of the United Nations Global Counter-Terrorism Strategy. The Office works closely with Member States; United Nations entities; civil society; international and regional organizations; academia; and other stakeholders, to strengthen existing and develop new partnerships to effectively prevent and counter terrorism.

UNOCT also works in close collaboration with the Security Council subsidiary bodies mandated to enhance the capacity of Member States to prevent and respond to terrorist acts, which include: the Counter-Terrorism Committee (CTC); the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities; as well as the Security Council Committee established pursuant to resolution 1540 (2004). The committees are supported in their work by different entities; CTC has its Executive Directorate (CTED) to carry out its policy decisions and conduct expert assessments of Member States, whereas the 1267 Committee has its Monitoring Team.

Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS Programme)

The AROS Programme, led by UNOCT, was launched in 2021 to raise awareness on and promote the exchange of good practices and guidance related to AROS, including unmanned aircraft systems (UAS); enhance the capacity of Member States to investigate and counter terrorist threats related to AROS, including UAS; and enhance the capacity of Member States to use AROS, including UAS, in compliance with their obligations under international law.

The AROS Programme supports key General Assembly resolutions, including the United Nations Global Counter-Terrorism Strategy (resolution 60/288) and its eighth review (resolution 77/298). The Programme is also responsive to Security Council resolutions, including resolutions 2309 (2016), 2341 (2017) and 2370 (2017); CTC and CTED identified priorities; and the 2018 Global Counterterrorism Forum, Berlin Memorandum.

The Programme is implemented in partnership with the United Nations Global Service Centre, Conflict Armament Research (CAR), CTED and the International Civil Aviation Organization (ICAO), in collaboration with several United Nations and global counter-terrorism compact entities, the private sector and civil society organizations.

Conflict Armament Research

Since 2011, CAR has established active field investigation capabilities to track weapons and military assistance supply networks in over 25 conflict- and terrorism-affected environments globally. Its investigation teams work on the ground in active armed conflicts alongside national defence and security agencies.

The teams document weapons and other related materiel including UAS at the point of use and track their sources back through the chains of supply. Its teams investigate weapons in a variety of conflict related situations – be they recovered by State security forces, surrendered at the cessation of hostilities, cached or held by insurgent forces. All CAR data are housed in iTrace®, a European Union and German Government-funded project that provides policymakers with precise, verified information required to understand weapon transfers in detail and, thereby, to develop effective, evidence-based weapon management and control.

About the research team

ROB HUNTER-PERKINS is the Head of Research at Conflict Armament Research (CAR). Prior to joining CAR in February 2018, he worked with several non-governmental organizations in the field of arms control and humanitarian disarmament; between 2015 and 2017, he was the senior researcher for the Arms Trade Treaty Monitor project, tracking global implementation of the Treaty. He holds a master's degree from the Post-war Reconstruction and Development Unit at the University of York, United Kingdom.

HIMAYU SHIOTANI is the Head of International Policy at CAR. Prior to this, he was Head of the Conventional Arms Programme at the United Nations Institute for Disarmament Research (UNIDIR) and a research associate at the James Martin Center for Nonproliferation Studies in Monterey, California, United States. He holds a master's degree in international policy studies, with a certificate in non-proliferation studies from the Middlebury Institute of International Studies, and has authored numerous publications.

DR. JAMES ROGERS is the incoming Executive Director of the Cornell Brooks Tech Policy Institute at Cornell University. He was previously the DIAS Associate Professor in War Studies at the Centre for War Studies at the University of Southern Denmark. He was also an Associate Fellow of LSE IDEAS at the London School of Economics, and a Defence Opinion Leader at the Ministry of Defence of the United Kingdom. Between 2018 and 2021, he acted as weapons adviser to the United Nations Special Rapporteur on extrajudicial, summary or arbitrary executions. He is a TEDx speaker, presents the Warfare podcast and is the author of Precision: A history of American Warfare, forthcoming in December 2023.

Acknowledgements

The present report is the product of a joint research initiative – between the Autonomous and Remotely Operated Systems (AROS) Programme of the Special Projects and Innovation Branch within the Office of Counter-Terrorism (UNOCT), and Conflict Armament Research (CAR) – on the use of unmanned aircraft systems for terrorism-related purposes. The AROS Programme team included Khalil Otmane (Programme Manager), Nigel Lazarus (Programme Coordinator), Maximilien Mougel, Ellie Roberts, Kamal Anwar and Akvile Ginotiene. The joint research initiative was funded by the generous contributions of the United Arab Emirates.

The initiative was also made possible thanks to the contributions and collaboration of the programme's implementing partners, including the United Nations Global Service Centre, under the Department of Operational Support; the Counter-Terrorism Committee Executive Directorate; the International Civil Aviation Organization; and non-implementing partners including the unmanned aircraft systems Joint Cell; the Department of Political and Peacebuilding Affairs; the Department of Peace Operations; the Office for Disarmament Affairs; the International Atomic Energy Agency; the European Commission; the International Criminal Police Organization (INTERPOL); the World Customs Organization; Skydio; TEKEVER; as well as a panel of academic experts who reviewed this report and provided critical feedback.

Abbreviations and acronyms

AI	artificial intelligence
AROS	autonomous and remotely operated systems
CAR	Conflict Armament Research
CBRN	chemical, biological, radiological or nuclear
CJNG	Jalisco New Generation Cartel
CTC	Counter-Terrorism Committee
CTED	Counter-Terrorism Committee Executive Directorate
ICAO	International Civil Aviation Organization
IED	improvised explosive device
INTERPOL	International Criminal Police Organization
MANPADS	man-portable air defence system
NATO	North Atlantic Treaty Organization
UAS	unmanned aircraft system
UAV	unmanned aerial vehicle
UNAOC	United Nations Alliance of Civilizations
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNIDIR	United Nations Institute for Disarmament Research
UNOCT	Office of Counter-Terrorism
WCO	World Customs Organization

Key findings

ACQUISITION

Trends

- The three most reported acquisition types were commercial procurement, illicit trafficking and illicit manufacture or modification.
- Non-State armed groups often pursue multiple acquisition strategies in order to access unmanned aircraft systems (UAS). The approaches identified in this report may therefore be regarded as mutually reinforcing.

Outliers

- The least frequently reported acquisition types by Member States related to the loss or diversion of UAS from authorized custodians. This encompasses losses both "static" (i.e. theft from private or national holdings) and "dynamic" (i.e. abandonment or capture from active deployment).

Priorities

- Member States expressed the view that efforts should be focused on the multilateral level, on upholding norms against provision of UAS capabilities to non-State armed groups.
- Member States emphasized that access to unregulated or loosely controlled commercial technology was a critical driver of UAS acquisition by non-State armed groups.
- Several Member States raised concerns regarding border control and the continuation of illicit trafficking, including the use of UAS to conduct trafficking.

WEAPONIZATION

Trends

- The two most reported modification types encountered in this study were the addition of potential weaponization facilitators such as high-end cameras, or release mechanisms, and the integration of an explosive payload, either with conventional munitions or improvised explosives.

Outliers

- Some Member States reported that there had been actual or attempted weaponization of UAS to include a dispersal or spraying mechanism, which could allow for the spreading of chemical or biological agents.

Priorities

- The most prominently expressed priority area of focus for countermeasures was modes of modification that would enable direct kinetic attacks using UAS, especially the threat of lethal use of UAS armed with an explosive payload.
- Member States also highlighted challenges from emerging and fast-evolving technological advances, such as increased flight and targeting autonomy as a result of artificial intelligence (AI), or the integration of more powerful engines and flight capabilities to enable UAS to effectively evade countermeasures.

DEPLOYMENT

Trends

- Member States indicated that they had experienced attacks, disruption or other incidents involving the use of UAS by non-State armed groups. Such incidents were not centralized in any one region, and they did not take place solely in countries affected by active armed conflict.
- The most common form of reported non-State armed groups deployment of UAS was to gather intelligence, surveillance and reconnaissance. The second reported deployment type is disruption and interference of critical infrastructure, such as energy utilities and transport sites.

Outliers

- The least observed forms of UAS deployment included electronic/signal operations and swarm attacks. These deployment types may reflect advance capabilities outside the reach of most non-State armed groups and requiring a significant level of expertise to deploy. Nonetheless, these deployment types were reported by Member States as areas of growing concern.

Priorities

- Two key concerns emerged during consultations for this report. The first is the use of UAS to carry out direct kinetic attacks, particularly the use of improvised explosive devices or dropping of conventional munitions. Within this, a threat dynamic that was highlighted as a particular concern was the use of UAS in targeted killings of high-value, high-profile and high-status individuals.
- The second concern is the increasing use of UAS by non-State armed groups to target maritime vessels and infrastructure, including ports.

I. Background

Rise of the non-State threat of UAS

The ability of non-State armed groups to acquire, weaponize and deploy unmanned aircraft systems (UAS) presents a significant threat to international peace and security and to the protection of civilians and civilian objects. In recent years, terrorism has become notably more diffuse and diverse in nature, aided in part by the adoption of new and emerging technologies, such as UAS.[1] (A glossary of key terms used in this study is presented in box 1.) Non-State armed groups use UAS to conduct a wide range of activities that pose a security threat, including for terrorism-related purposes (e.g. attacks against, and incursions into, vulnerable targets, including critical infrastructure or public places ("soft targets")); for intelligence, surveillance and reconnaissance; for targeting support; and for illicitly trafficking commodities such as drugs, arms and explosives. Some examples of these diverse deployment types are listed in table 1.

In 2020, the Special Rapporteur on extrajudicial, summary or arbitrary executions noted in her report to the Human Rights Council that at least 20 non-State armed groups had reportedly obtained armed and unarmed UAS.[2] A subsequent comprehensive review estimates that 65 criminal, insurgent or terrorist organizations now have this ability.[3] The Global Terrorism Database shows a sharp increase in incidents of non-State UAS use since the early 2000s, with 65 attacks in 2020 alone.[4] Conflict Armament Research (CAR) field investigators have documented non-State use of UAS in several contexts and reported on the international supply chains underpinning these groups.[5]

In 2023, the United Nations monitoring team concerning Da'esh, Al-Qaida and associated individuals, groups, undertakings and entities reported on four notable trends: (1) more terrorist groups have developed UAS capabilities; (2) some terrorist groups are actively seeking to identify new avenues for acquisition and advancement of UAS capabilities; (3) some terrorists groups are sharing technology and training on the use of UAS; and (4) the use of UAS by terrorist groups continues to proliferate globally.[6] United Nations arms experts monitoring the implementation of relevant Security Council sanctions have identified the non-State use of

1. General Assembly resolution 77/298.
2. A/HRC/44/38.
3. This figure is derived from ongoing research by Chávez and Swed (2021). See also Rogers (2022) and Chávez and Swed (2023a).
4. According to a keyword search for "drone" on the Global Terrorism Database conducted on 9 May 2023.
5. More information on CAR field investigations is available at www.conflictarm.com.
6. S/2023/549.

UAS in the Democratic Republic of the Congo,[7] Mozambique,[8] Somalia,[9] Yemen,[10] and in the West Africa region,[11] while indications of growing UAS capability as well as intent of non-State armed groups to acquire and deploy UAS have been reported in Afghanistan,[12] Libya[13] and the Syrian Arab Republic.[14]

Technology that was once either exclusively the preserve of a limited number of States, or else prohibitively expensive for commercial and civil actors, has become readily available. The democratization of access to UAS has resulted in immeasurable societal benefits. In the United Nations context alone, UAS are now used to gather data in the wake of natural emergencies and disasters, support peacekeeping missions to protect civilians in armed conflict, and deliver life-saving medicine and vaccines to otherwise inaccessible communities.[15] This dramatic shift in the global proliferation of UAS technologies, however, also increases the likelihood of UAS being misused, including for terrorism-related purposes, or that they will be diverted for use in multiple illicit activities. At the same time, UAS capabilities are rapidly advancing, and commercially available systems now vastly outstrip those available a decade ago.

BOX 1: KEY TERMS

- **Non-State armed group**: This term is widely used, and its definition varies.[a] This report broadly applies the term "non-State armed groups" to describe unauthorized groups and recipients associated or involved in the acquisition, weaponization and use of UAS, including for terrorism-related purposes. A range of non-State armed groups have used, or sought to use, UAS. Diverse non-State armed groups, while differing in motive and purpose, may overlap as regards UAS modalities of acquisition. The European Union Aviation Safety Agency has categorized a range of different intents behind pilots of unauthorized UAS, including careless and clueless individuals, activists and protesters, and criminal and terrorist use.[b]

7. In March 2021, the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO) reported the presence of an unmanned aerial vehicle (UAV) flying near a new camp of the Allied Democratic Forces in the Democratic Republic of the Congo. Six ex-combatants and/or former abductees confirmed the presence and use of at least two surveillance UAVs by the Allied Democratic Forces (see S/2021/560 and S/2023/431).
8. The authorities in Mozambique have reported shooting down two Ahlu Sunna wal-Jama'a surveillance UAVs (see S/2023/95).
9. "In Somalia, there is prolific use of [remotely piloted aircraft systems], including mini-drones, by Al-Shabaab" (S/2022/547).
10. "The Houthi forces continue to deploy small- and medium-sized unmanned aerial vehicles in various roles, ranging from reconnaissance use to their use as loitering munitions, i.e. as so-called 'suicide or kamikaze drones'" (S/2019/83).
11. Jama'a Nusrat ul-Islam wa al-Muslimin, Islamic State in the Greater Sahara, and Islamic State in West Africa Province have reportedly used reconnaissance UAS for surveillance (see S/2023/95).
12. See the fourteenth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2665 (2022) concerning the Taliban and other associated individuals and entities constituting a threat to the peace stability and security of Afghanistan (S/2023/370).
13. See S/2023/549.
14. Ibid.
15. UN News (2017).

- **Unmanned aircraft system (UAS)**: The International Civil Aviation Organization (ICAO) defines UAS as "an aircraft and its associated elements which are operated with no pilot on board".[c] In this report, the term describes a system whose components include the necessary equipment, network and personnel to control an unmanned aircraft. UAS are remotely piloted, pre-programmed or controlled vehicles that can perform an array of tasks such as surveillance, reconnaissance and targeting support.[d]
- **Unmanned aerial vehicle (UAV)**: The airborne components of UAS, a UAV consists of the airframe, the navigation system, the power system and the payload.[e] UAVs span a wide range of sizes and capabilities, and there is no universal classification of UAVs.[f]
- **Acquisition**: This term refers to any process through which non-State armed groups access UAS, UAS components or UAS technology.
- **Weaponization**: This term refers to a process whereby non-State armed groups modify UAS already in their possession to increase their capability to carry out attacks.
- **Deployment**: This term refers to the operational objectives and targets in which non-State armed groups seek to use UAS.

a. As a reference, the Integrated Disarmament, Demobilization and Reintegration Standards (IDDRS) defines "armed groups" as "a group that has the potential to employ arms in the use of force to achieve political, ideological or economic objectives; is not within the formal military structures of a State, State-alliance or intergovernmental organization; and is not under the control of the State(s) in which it operates" (see www.unddr.org/modules/IDDRS-1.20-Glossary.pdf).
b. European Union Aviation Safety Agency (2021).
c. ICAO (2011).
d. This definition is taken from the "Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017)" (the guidelines cite the US Department of the Army, Techniques for Combined Air Defense, US FM ATP 3-01.8 (2016)).
e. Ibid. Although the term "drone" is often used as shorthand, ICAO considers drones to be a subset of unmanned aircraft.
f. Grand-Clément and Bajon (2022a). NATO categorizes UAS into three dedicated classes, according to their maximum take-off weight and operating altitude. These classes span from small, commercially available craft, to advanced military-grade systems. Unless explicitly stated, this report has not made a distinction between different UAV classes. See, for example, United Kingdom, Ministry of Defence (2017).

International efforts to address the terrorist threat of UAS

Pursuant to Security Council resolution 1373 (2001), Member States are required to refrain from providing any form of support to entities or persons involved in terrorist acts, including by eliminating the supply of weapons to terrorists. Denying access to weapons is a complex and multifaceted challenge, however, due in large part to the rapidly evolving nature of the operational terrorist environment. In 2017, the Counter-Terrorism Committee (CTC) held an open briefing on preventing terrorists from acquiring weapons. Subsequently, the Security

Council unanimously adopted resolution 2370 (2017), which calls on all Member States to eliminate the supply of weapons – including small arms, military equipment, UAS and their components, and improvised explosive device (IED) components – to those involved in terrorist acts. It specifically encourages Member States to prevent and disrupt procurement networks for such weapon, systems and components to and between actors involved in terrorist acts. It was the first Security Council resolution specifically dedicated to addressing this link.[16]

Since the adoption of resolution 2370 (2017), UAS have been identified as a key terrorist threat by CTC. A growing number of associated multilateral frameworks and guidance increasingly recognize the threat of non-State use of UAS and seek to promote coordinated actions to address this.

In October 2022, CTC in its special meeting in New Delhi, India, adopted the Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes.[17] The Declaration is significant in a number of ways for multilateral efforts to address the UAS threat posed by non-State armed groups. First, CTC strongly condemned the continued flow of UAS to terrorists, illegal armed groups and criminals. It encouraged Member States to address the threat posed by the use of UAS for terrorist purposes, including by preventing and disrupting procurement networks for such weapons, systems and related components. Second, it took stock of notable international efforts that contributed to raising awareness of, and preparedness against, the threat posed by the use of UAS for terrorist purposes. Third, CTC decided to work on recommendations pertaining to the threats posed by the misuse of UAS by terrorist actors after the conclusion of the special meeting as one of the three key CTC thematic priorities. CTC further expressed the intention to develop, with the support of the Counter-Terrorism Committee Executive Directorate (CTED), a set of non-binding guiding principles to assist Member States in countering the threat posed by the use of new and emerging technologies for terrorist purposes. This effort is expected to include compiling good practices on the opportunities offered by the same set of technologies to counter the threat, consistent with international human rights and international humanitarian law.

CTC seeks to pursue such follow-on actions – taking into account the need to balance fostering innovation and preventing the use of UAS for terrorist purposes – as the applications and accessibility of UAS and associated components continue to expand in the public and private sectors.

Additionally, during the eighth review of the Global Counter-Terrorism Strategy, conducted in 2023 and approved by the General Assembly, Member States expressed concern over the proliferation and democratization of emerging technologies, including UAS (and weaponization of commercial drones), and condemned the movement of such systems and related components for terrorist purposes.[18] The Strategy provides an essential framework for strengthening cooperation among States and other relevant stakeholders to prevent the acquisition of weapons by terrorists, including UAS.

16. UAS concerns have been recognized by other relevant Security Council resolutions, including 2395 (2017), 2462 (2019), 2482 (2019) and 2617 (2021).

17. CTC (2022).

18. General Assembly resolutions 77/298 and 75/291.

Furthermore, the Global Counterterrorism Forum published a set of non-binding good practices in 2019, known as the Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems.[19] The Memorandum seeks to inform and guide Governments in identifying, developing and refining policies, practices, guidelines, regulations, programmes and approaches for countering the terrorist use of UAS. The Memorandum identifies 26 good practices in four key areas for States: (1) assessing the risk, assessing vulnerabilities and raising awareness; (2) enhancing information-sharing, engaging with relevant stakeholders and educating the public; (3) implementing policies and regulations and establishing crisis planning; and (4) developing tactical countermeasures and technical solutions.

Table 1
Examples of UAS attacks involving non-State armed groups, including for terrorism-related purposes*

Year	Country	Non-State armed group	Deployment type
1993	Japan	Aum Shinrikyo	Planned attack to spread sarin gas using remotely controlled helicopters.
2002	Colombia	Fuerzas Armadas Revolucionarias de Colombia (FARC)	Nine model aeroplanes recovered by the Colombian military, believed to have been used to smuggle drugs.
2006	Israel	Hizbullah	Three small UAVs launched into Israel carrying 40-50 kg explosive payload, shot down by the Israeli Air Force.
2015	Japan	Environmental activist	A UAV carrying radioactive material landed on the roof of the Prime Minister's office in a protest against government policy.
2016	Iraq	Da'esh	Between 30 September 2016 and 11 February 2018, researchers identified 338 reports of UAV use by Da'esh in Iraq and the Syrian Arab Republic, of which 262 involved offensive action. This included the use of "booby trapping" UAVs to explode on recovery, deploying them as one-way attack UAVs, and use to guide vehicle-borne IED attacks, among others.
2018	Mali	Jama'at Nusrat al-Islam wal-Muslimin (JNIM)	Commercial UAVs used to record propaganda footage. In 2019, Algerian security forces seized 11 UAVs alongside a large number of explosives and conventional mortars.
2018	Bolivarian Republic of Venezuela	Military defectors	Commercial UAVs carrying explosives used in the attempted assassination of President Nicolás Maduro.
2018	Syrian Arab Republic	Hay'at Tahrir al-Sham	Multiple customized UAVs used in a rudimentary "swarm" in an attack on a military base.
2019	Yemen	Ansar Allah	A UAV detonated above a military parade, killing multiple people.
2019	China	Criminal groups	UAVs reportedly used to drop contaminated pork products to fake outbreaks.
2022	Syrian Arab Republic	Hay'at Tahrir al-Sham	A single-use, fixed-wing UAV rigged with explosives flown into a church, killing two people.
2022	United Arab Emirates	Ansar Allah	Attack strikes three oil transport tankers, killing several workers and sparking a fire at Abu Dhabi's international airport.

Sources: Batrawy (2022); BBC News (2015); Dass (2022); Gibbons-Neff (2016); Haugstvedt (2021); Hoenig (2014); International Crisis Group (2018); Paton Walsh and others (2019); Rassler (2016); Reuters (2016); Veilleux-Lepage and Archambault (2022); Waters (2019); Weiss (2018); Zhang and Daly (2019).

* The examples are drawn from a review of existing literature and expert sources. The examples were selected to illustrate how non-State armed groups have sought to deploy UAS in recent years, and to reflect the breadth of geographical contexts affected. It is not exhaustive, and in some cases, although the incidents are claimed or commonly attributed to a non-State armed group, responsibility is still disputed or unproven.

19. Available at www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fI%3D&portalid=1.

Operationalizing UAS frameworks

Efforts to operationalize these frameworks and guidance continue. Notably, recent multilateral initiatives to assist States in their effort to counter the threat posed by UAS acquisition and use by non-State armed groups include the following.[20]

- In 2022, the release of the "Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons", in particular its submodule on preventing terrorists from acquiring UAS and their components. The guidelines were developed within the framework of the United Nations Global Counter-Terrorism Coordination Compact Working Group on Border Management and Law Enforcement relating to Counter-Terrorism, and were compiled by CTED, the Office of Counter-Terrorism (UNOCT) and the United Nations Institute for Disarmament Research (UNIDIR). Organized as "upstream" preventative measures and "downstream" response measures, this submodule seeks to support States in their preparedness against the threat of UAS posed by non-State armed groups (the measures areas identified in the guidelines are shown in table 2). A series of follow-on awareness-raising and capacity-building activities are currently being implemented by several United Nations entities.
- In 2022, the release of a specialized module on "Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS): good practices guide" by the UNOCT Global Programme on Countering Terrorist Threats against Vulnerable Targets, which builds on "The protection of critical infrastructure against terrorist attacks: compendium of good practices", [21] developed by CTED, UNOCT and the International Criminal Police Organization (INTERPOL) in 2018 and updated in 2022.[22]
- The United Kingdom and the United States are currently cooperating under the Global Counterterrorism Forum to operationalize the Berlin Memorandum to bring greater awareness and build a network forum of experts to better understand the best practices for countering malign and illicit uses of UAS, while balancing and understanding the commercial benefits of its use.
- Since 2015, ICAO has undertaken efforts to strengthen guidance and provisions that can be used by States to regulate UAS. Those efforts include the development and maintenance of the ICAO Aviation Security Manual, the launch of a public "UAS Toolkit", which is a compilation of best practices and regulations in support of States' efforts to develop effective operational guidance on the use of UAS. In addition, ICAO has created model UAS regulations designed to support States in establishing and refining their national guidelines for domestic UAS operations.[23]

20. In addition, there are series of regional and national initiatives in this area of work. Some are highlighted in relevant sections of the present report.

21. Available at www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf.

22. The specialized module was produced by UNOCT in partnership with CTED, United Nations Alliance of Civilizations (UNAOC) and the United Nations Interregional Criminal Justice Research Institute (UNICRI). See www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf.

23. See www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx.

Table 2
United Nations multidimensional response measures to the threat posed by UAS

	Upstream		Downstream
1.	**National policy, legislation, regulation and administrative procedures**	**1.**	**Counter-UAS systems and techniques**
1.1.	– National policy or strategy		
1.2.	– National coordinating entity and coordination mechanisms		
1.3.	– National legislation and regulations		
1.4.	– National technical standards		
2.	**Capability, normative and operational development for countering UAS**	**2.**	**UAS incident scene: safety and security**
3.	**Considerations pertaining to specific areas and activities**	**3.**	**Recovery and preservation of evidence**
3.1.	– Customs and border control		
3.2.	– Control of UAS and key subsystems		
4.	**Law enforcement intelligence-led operations**	**4.**	**Technical exploitation of recovered UAS and components**
5.	**International and regional cooperation, including information-sharing**	**5.**	**Information management**
		6.	**Identification of perpetrators**
		7.	**Criminal justice process**
		8.	**Development of UAS countermeasures**

Source: Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017).

BOX 2: ARMS CONTROL AND NON-STATE USE OF UAS

Currently, there is no multilateral arms control mechanism dedicated to addressing threats posed by UAS comprehensively.[a] However, several multilateral arms control regimes are relevant to UAS, focusing either on regulating the transfer of armed UAS and related components, or on promoting transparency in transfers. Notable regimes include the following.[b]

- **Security Council resolution 1540 (2004)**: States have expressed concern about the use of UAS and components by non-State armed groups as a delivery vehicle for chemical, biological and radiological agents. Resolution 1540 (2004) decided that States should adopt and enforce appropriate effective laws that prohibit any non-State armed group from manufacturing, acquiring, possessing, developing, transporting, transferring or using nuclear, chemical or biological weapons, and their means of delivery, which include unmanned delivery systems.[c]

- **Missile Technology Control Regime**: As an informal framework established to promote the non-proliferation of systems that could be used for the delivery of weapons of mass destruction (such as missiles, UAS and related technologies), the Regime consists of voluntary guidelines that help participating States to restrict national exports of armed and unarmed UAS above a certain technical threshold, distinguishing between UAS of the greatest sensitivity (Category I) and risky items (Category II), as well as related equipment, components and production facilities specifically designed for these systems.[d]

- **Wassenaar Arrangement**: Serving as an export control regime for conventional and dual-use goods and technologies, the Wassenaar Arrangement contains two lists: (a) List of Dual-Use Goods and Technologies; and (b) Munitions List.

BOX 2 (*CONTINUED*)

Together, the lists capture armed UAS and their components, making these subject to national transfer controls by participating States, and specific transparency requirements depending on their sensitivity.[e]

- **United Nations Register of Conventional Arms**: Intended to promote transparency in transfers and holdings of conventional arms, the register encourages States to provide, on a voluntary basis, information about the number of arms they import and export in seven categories, including combat aircraft and unmanned combat aerial vehicles (Category IV) and attack helicopters (Category V).[f]
- **Arms Trade Treaty**: As an international legally binding instrument, the Arms Trade Treaty regulates international transfers of conventional arms, including certain categories of UAS applicable under the scope of the Treaty (article 2.1(d)) and description under general implementation (article 5.3). It establishes provisions for States Parties to apply the Treaty's prohibitions and export assessment obligations to armed UAS transfers, and to report on their authorized or actual exports in their annual reports.[g]

Although existing arms control regimes provide policies, standards and practical measures to regulate the transfer of certain types of UAS, primarily by States, and to reduce their risk of diversion, membership and adherence to these mechanisms vary considerably, as do the provisions of the mechanisms themselves. They do not necessarily share the scope of systems and components, key terms and concepts, presenting a fragmented landscape for addressing a wide range of threats and challenges posed by UAS, including in the context of non-State acquisition and use. In 2017, research conducted by UNIDIR concluded that there was an urgent need to pursue a multilateral process aimed at developing standards and principles around the use of UAS, including the regulation of acquisition of relevant components, under the auspices of the United Nations.[h]

a. See Borrie, Finckh and Vignard (2017).
b. For a more comprehensive overview of relevant arms control regimes, see ibid., appendix 2.
c. See www.un.org/en/sc/1540.
d. See www.mtcr.info.
e. See www.wassenaar.org.
f. See www.unroca.org/categories.
g. See https://thearmstradetreaty.org/treaty-text.html#.
h. Borrie, Finckh and Vignard (2017).

Despite the existence of relevant multilateral counterterrorism and arms control frameworks, efforts to develop multilateral norms and standards applicable to non-State use of UAS are best characterized as at an early-to-maturing stage. There is currently no comprehensive, binding framework specifically dedicated to addressing the threat posed by UAS acquisition and use by non-State armed groups, including terrorists, at the multilateral level. This presents a notable policy gap.

This gap, combined with the recognition of increased proliferation and misuse of UAS, as well as the rapidly evolving UAS technology landscape concurrently with other technological advancements (such as AI) and related countermeasures, has led to recent debate on the need for a dedicated international agreement to control UAS proliferation specifically to prevent acquisition and use for terrorist purposes.[24]

Methodology

About this project

A thorough understanding of the trends in the acquisition, weaponization and deployment of UAS and related components by non-State armed groups is a prerequisite to ensuring that awareness-raising and technical assistance efforts can be implemented in a meaningful, effective and coherent manner. To that end, the UNOCT Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS Programme) and CAR have produced the present report on the global acquisition, weaponization and deployment of UAS by non-State armed groups. This report is the first scoping of Member States' priorities and experiences of non-State use of UAS. It constitutes an initial overview and a snapshot of trends as identified by experts and operational personnel of Member States working to counter this threat.

This report represents a key contribution of the multi-year AROS Programme designed to enhance the capacity of Member States to prepare for, investigate, counter and mitigate AROS-related risks and threats; to use AROS, including UAS, in compliance with their obligations under international law; to promote global coordination and the exchange of expert best practices, and guidance with regard to the benefits and threats associated with such capabilities. It also draws on the evidence gathered by CAR field investigation teams in conflict- and terrorism-affected environments since 2011 to document and trace the supply of UAS and UAS components, among a broader range of conventional and non-conventional military materiel, to illicit non-State armed groups.

Purpose of this report

This report seeks to contribute to existing efforts to establish a global baseline of national experience of the threat of UAS use by non-State armed groups. It highlights current overarching trends in how actors acquire, weaponize and deploy UAS. It also raises outlier practices that may signal emerging threats and identifies priority concerns of Member States.

This report therefore seeks to contribute to increased awareness of the threat of UAS proliferation and potential use for terrorism-related activities, and to enhance the knowledge of Member States on preparedness to prevent and reduce UAS-related threats posed by non-State armed groups, including terrorists. The research focuses on understanding key trends and developments relating to four main areas: (1) acquisition; (2) weaponization; (3) deployment; and (4) prevention and countermeasures.

The knowledge generated is made available to help better inform capacity-building efforts, and ongoing multilateral discussions among States on ways to further strengthen preventative

24. See, for example, Rogers (2022).

and mitigation measures against the terrorist acquisition of components that can be used to produce and deploy UAS.

This report presents an initial collection of views from Member States on this topic and constitutes an exploratory survey of expert experience. UNOCT and CAR intend to build on, and learn from, these findings in future research – including through research on further global trends – in order to assess how the threat of non-State use of UAS evolves and therefore inform effective mitigation and prevention strategies.

BOX 3: RESPECTING HUMAN RIGHTS IN THE PREVENTION AND MITIGATION OF TERRORIST ACQUISITION AND USE OF UAS AND COMPONENTS

In Security Council resolution 2370 (2017), paragraph 13, Member States are urged to respect human rights and fundamental freedoms in the course of their efforts to prevent terrorists from acquiring weapons, including UAS and UAS components. The "Technical guidelines to implement resolution 2370" highlight several example areas where States have an obligation to comply with international human rights law in the course of countering terrorist uses of UAS. These include preventing, combating and punishing criminal acts, or developing capabilities to counter UAS acquisition and use. The guidelines, in pp. 45 and 46, note that in all such measures, States must respect their obligations under applicable domestic law and international law, including international human rights law, and ensure that the right to life and the protection of civilians are priorities in any environment and under any circumstances.

Research process

In 2022 and 2023, UNOCT and CAR undertook extensive consultations with Member States to gather information, knowledge and expertise relating to the use of UAS by non-State armed groups. The research partners developed a qualitative analysis of the experiences and concerns of key stakeholders, focusing especially on Member States. The research process included interviews with Member States, United Nations entities, intergovernmental organizations, civil society and the private sector; a questionnaire to all Member States; and a three-day regional consultation with Member States. Each research activity is described below.

The project identified three main information sources: technical and policy experts from Member States, specialist entities including industry and academia, and field investigation data collected by CAR. Researchers developed a list of overarching guiding questions that formed the basis of data-collection efforts.

Acquisition

- What types of UAS are non-State armed groups acquiring, and how are they doing so?
- How are non-State armed groups cooperating across borders to secure access to UAS?
- How effective are existing controls in preventing illicit actors from accessing UAS, and what relevant safeguards and preventive measures exist to deter non-State acquisition efforts?

Weaponization

- What types of emerging technological developments in the weaponization of UAS are of the greatest concern to Member States?
- How are commercial UAS being modified to make them more dangerous or effective?
- How are non-State armed groups sourcing the material, equipment and knowledge needed to adapt and weaponize systems in their possession?
- What measures can Member States take to practically prevent non-State armed groups from attempting to weaponize commercial UAS?

Deployment

- What are the operational priorities that non-State armed groups might look into to deploy UAS?
- How can concerned stakeholders map the context of current and potential non-State use of UAS to inform deterrence and mitigation strategies?
- What policies, procedures and coordination efforts exist to counter the proliferation and threat posed by the non-State use of UAS?

These questions provided the framework to guide research efforts. The project identified three primary data-collection avenues:

- A questionnaire issued to all Member States and shared with international organizations
- Regional expert consultations with Member States
- Interviews with specialist entities.

Questionnaire

The questionnaire issued to Member States is presented in the annex to this report. The questionnaire consisted of 12 sections comprising 47 questions. They included multiple choice questions (respondents can select from a list of options, including "other"), as well as open text questions (respondents were invited to provide further details as appropriate and relevant). Apart from the sections on respondent details and confidentiality, the questionnaire centred on six areas:

1. National experience of non-State use of UAS
2. UAS acquisition
3. UAS weaponization
4. UAS deployment
5. Counter-UAS policies and controls
6. Counter-UAS exploitation and UAS digital forensics.

The questionnaire was made available to respondents in August 2022. A cut-off date of 28 February 2023 was set for the inclusion of initial responses in the analysis for this report. Participation remains open to all interested Member States, which can be accessed at conflictarm.org/UAS_Questionnaire. Member States were notified about the questionnaire via a note verbale. Completing the questionnaire was a voluntary, self-reporting exercise carried out by representatives of Member States, and responses were not subject to additional verification by the research team.

As at 28 February 2023, the questionnaire was completed by 40 respondents, representing 21 Member States and four international organizations.[25] In several cases, there were multiple respondents from the same State.[26] In addition, the questionnaire was completed by the European Commission, the Department of Operational Support, the World Customs Organization (WCO) and another United Nations entity that requested not to be identified.

Table 3 presents a list of the States that responded to the questionnaire, organized by region: Africa (6); Americas (5); Asia-Pacific (7); Europe (3).[27] Three States from the Americas and two States from Asia-Pacific asked not to be identified.

Table 3
Respondent States, by region

Africa	Americas	Asia-Pacific	Europe
Algeria	Argentina	Armenia	Portugal
Burkina Faso	Mexico	Cambodia	Switzerland
Ethiopia		India	Ukraine
Malawi		Palau	
Nigeria		Qatar	
Senegal			

This report anonymizes States' specific responses throughout in order to reflect on global trends and to respect the request of some States to withhold information relating to their national experience.

The questionnaire was primarily completed by representatives from a national defence and security agency (table 4), either the ministry of defence, an equivalent to the interior ministry, or a representative of a State's national intelligence service. In two States, the civil aviation authorities completed the questionnaire.

Table 4
Respondent entities

Entity type	No. of respondents	Regional breakdown
Civil aviation	2	Africa (1), Europe (1)
Defence or military	8	Africa (2), Americas (3), Asia-Pacific (2), Europe (1)
Foreign affairs	2	Africa (1), Americas (1)
Intelligence or counter-terrorism	5	Africa (1), Asia-Pacific (3), Europe (1)
Interior or other national security	6	Africa (1), Americas (2), Asia-Pacific (2), Europe (1)

25. Forty-seven participants started the questionnaire, but seven did not complete it, so were excluded in this analysis.

26. In six cases, multiple respondents from the same Member State completed the questionnaire. In three of those instances, the respondents represented different authorities within the country. Where at least one representative of a State has indicated a particular trend or issue in their national context, this has been included for analysis and reporting, even if this view was not consistently expressed by all respondents from that State. This is reflective of the differing exposure to, and experience of responding to, the non-State threat of UAS within a particular State.

27. For the purposes of this study, Member States were initially classified according to the United Nations Statistics Division regions (https://unstats.un.org/unsd/methodology/m49/). Member States from Asia and Oceania have been combined into the Asia-Pacific regional group.

Respondents were typically senior representatives of their department or agency, with specialist background in UAS and counter-terrorism. They included heads of counter-terrorism units in the national intelligence service; national security coordinators in the national interior ministry; wing commanders with the national air force; and chief inspectors with the national civil aviation authority.

Regional consultations

Between 25 and 27 January 2023, UNOCT and CAR convened a series of technical expert regional consultations. The consultations were held online and were conducted with simultaneous translation into the relevant United Nations languages. They were organized by region and were closed sessions, open only to Member States. The sessions were attended by over 400 participants from more than 30 Member States.

Each consultation consisted of two sessions. Session 1 focused on national and regional experiences, and priorities in addressing the threat of UAS-related terrorism. Session 2 explored the importance of policymaking in effectively preventing the acquisition, weaponization and deployment of UAS by non-State armed groups. Participants received the guiding questions for these expert consultations in advance, to facilitate active engagement and discussions.

Specialist entities

The research team conducted several expert interviews with representatives from relevant intergovernmental organizations. Researchers also conducted a literature review and drew on expert analysis and reporting by academics and civil society. These sources are included in the bibliography. Finally, the report includes several illustrative case studies derived from documentation of UAS conducted by CAR field investigators. CAR field investigation teams document illicit weapons, ammunition and related materiel in conflict-affected locations and trace their supply sources. Since 2011, CAR has operated in more than 25 conflict-affected environments, physically documenting all items and conducting formal weapon tracing and analysis to identify gaps within international supply chains. The case studies from CAR are distinctive in that they derive from physical documentation of seized UAS by field investigators. As CAR data collection is dependent on this physical access to materials, the case studies presented in this report are specific only to contexts in which field teams operate.

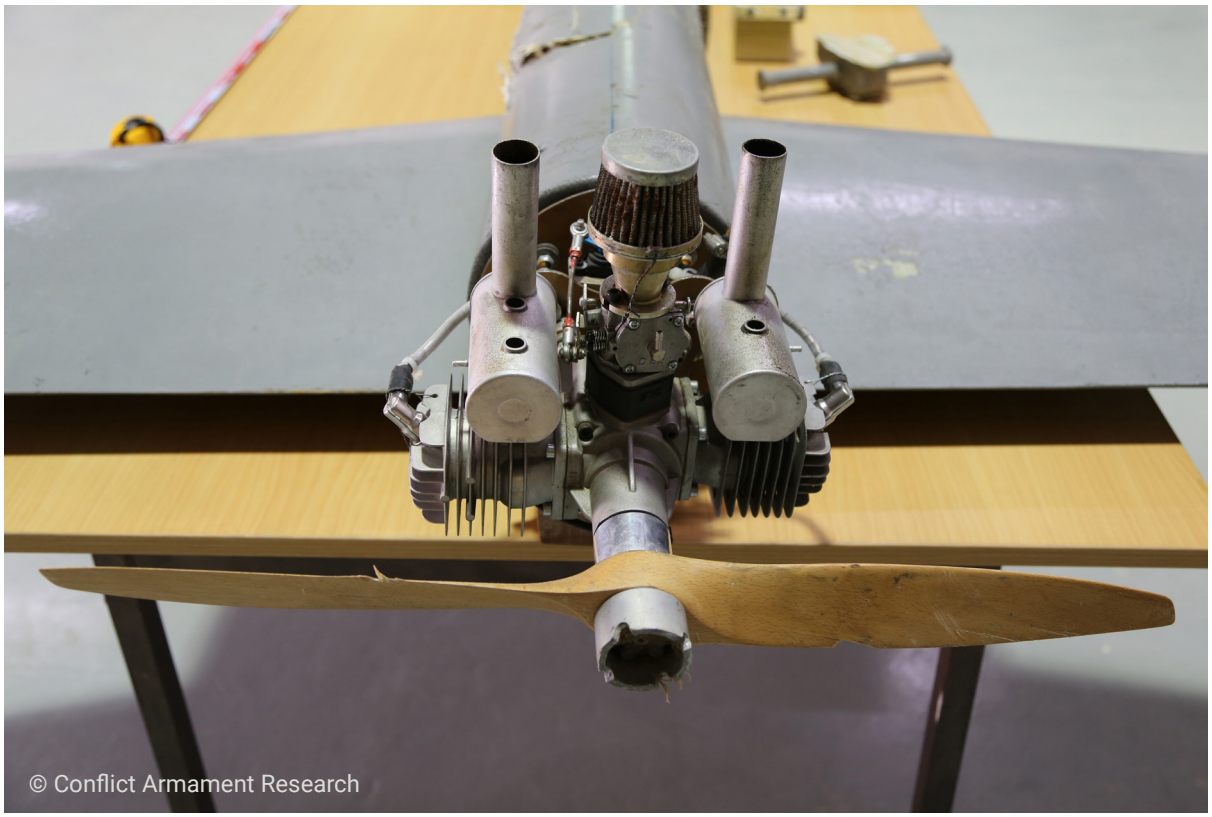
Limitations

Inputs received for this report are not representative of the experiences of all Member States. Therefore, any observation about a reported ”trend” should only be considered within the data collected by this study. Participation in the study was voluntary and at the discretion of each Member State.

The data collected in the study provides an initial snapshot of views expressed by participating Member States. UNOCT and CAR continue to invite interested Member States to share their experience and priorities by filling in the questionnaire, in order to build on the findings presented in this report and to provide a better understanding of the threat posed by the non-State use of UAS.

Figure 1

A close-up of the rear of a combat UAV, recovered from a non-State armed group by regional security forces (documented by CAR field investigators in February 2017)



II. Acquisition

Trends in acquisition

This section explores how non-State armed groups procure or otherwise gain access to UAS and UAS components. As part of this study, UNOCT and CAR presented Member States with a diverse range of acquisition approaches that might pertain to terrorist procurement of UAS technology. The term "acquisition" in this process refers to any process through which non-State armed groups, including terrorists, access UAS, UAS components or UAS technology. The questionnaire provided seven options, which were modified from a similar framework developed in 2021 to analyse diversion pathways related to conventional weapons and ammunitions.[28] These are defined in table 5, along with a full breakdown of States reporting attempted or actual acquisition through those means.

Table 5
Typology of acquisition of UAS

Acquisition type	Description	Breakdown	Total
Commercial procurement	Purchasing of commercial off-the-shelf products, components or related technologies, either lawfully or unlawfully.	Africa (3) Americas (4) Asia-Pacific (4) Europe (3)	14
Diversion from legitimate State or private custodians	Theft or loss from legal custodians, including manufacturers, private civilian owners or state holdings.	Africa (2) Americas (1) Asia-Pacific (2)	5
Illicit manufacture or modification	Self-design, development or assembly of UAS. This route to acquisition can refer to the manufacture of an entire system or the modification of one already in possession.	Africa (2) Americas (4) Asia-Pacific (3) Europe (1)	10
Illicit trafficking	Cross-border movement of materiel, including postal shipments and smuggling.	Africa (4) Americas (2) Asia-Pacific (4) Europe (1)	11
Loss from military or law enforcement during active use and deployment	Acquisition through forceful interception or capture of UAS from national security forces, government agencies, law enforcement or other stakeholders such as international peacekeepers. Loss also accounts for acquisition through abandonment or surrender of UAS.	Africa (1) Americas (1) Asia-Pacific (1) Europe (1)	4
State-sponsored diversion	A process by which a State backs a direct supply of UAS, UAS components or UAS technology to a terrorist or other non-State armed group.	Africa (2) Americas (2) Asia-Pacific (3) Europe (1)	8
Other	Acquisition types not addressed by the above definitions. States were invited to provide details about how non-State armed group operating in their State acquired – or attempted to acquire – UAS.	Africa (2) Americas (1) Asia-Pacific (1)	4

The list of acquisition types in table 5 is not exhaustive. As one State representative noted at the regional consultations in January 2023, "There is no single route of development for the use of drones by non-State armed groups, nor is there one pattern that they seem to

28. Malaret Baldo and others (2021).

follow; they seem to develop their drone capabilities in a manner that is quite unique to their logistical, political, strategic, tactical parameters. Unfortunately, this makes it more difficult for policymakers and analysts to understand the problem".

Furthermore, it is important to note that not all UAS types or classes are applicable to each acquisition type. Advanced military-grade UAS, for example, are not commercially available and are likely to be accessed only through specific pathways. Future research could build on this typology by integrating types of UAS. This typology is therefore intended as a first step towards developing a conceptual framework to understand how non-State armed groups, including terrorists, commonly access UAS technology and components. These fields are open to addition or amendment, especially as new or divergent procurement modalities become apparent.

The development of this nascent typology enables the mapping of common acquisition approaches. In so doing, this study seeks to support the formulation of appropriate countermeasures and the identification of effective intervention points. This study therefore establishes an initial baseline to understand the existing acquisition trends that are most observed by Member States, and which acquisition approaches are currently outliers or of limited relevance to UAS.

Terrorist and other non-State armed groups appear to pursue multiple acquisition strategies. States reported a mean average of 2.6 acquisition types. This supports the supposition that the different acquisition approaches are not exclusive to each other, but rather may be mutually reinforcing. Box 5 shows a case study in which multiple acquisition approaches have been pursued concurrently by the same non-State armed group. For example, nine of the 10 States that reported attempts made by non-State armed groups to illicitly manufacture UAS also reported at least one other acquisition mechanism, most commonly commercial procurement of UAS components.[29]

Four respondent States did not report observing any of these acquisition types.[30] Two States – both facing active and lengthy terrorist activity – responded affirmatively to all seven types. Notably, the questionnaire asked States to identify both actual and attempted acquisition of UAS. Responses provided by States did not specify whether these acquisition types had been successful, or whether they had failed or been disrupted by national countermeasures.

The three acquisition types most reported by the 21 respondent States were commercial procurement; illicit trafficking; and illicit manufacture or modification. Figure 2 shows the percentage of respondent States by region that reported experiencing a particular acquisition type. It shows regional commonalities and divergences. For example, four of the seven respondent States in Asia-Pacific reported commercial purchases as a procurement pathway used by non-State armed groups (see figs. 2 and 3), whereas all three respondents in Europe reported this.

29. The one exception was a State that reported the illicit manufacture of both UAS and UAS components by actors in their national territory.

30. Three of these States also reported that they did not have experience of active or attempted UAS use by non-State armed groups in their national territory.

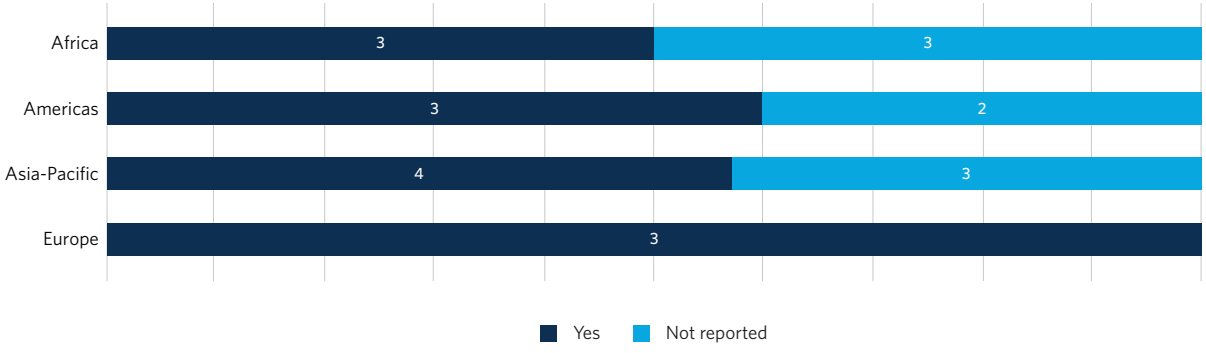
Figure 2
Percentage of respondent States by region that observed different acquisition types (n=21)

Acquisition type	Africa	Americas	Asia-Pacific	Europe
Commercial procurement	50%	80%	57%	100%
Diversion from legitimate state or private custodians	33%	20%	29%	0%
Illicit manufacture or modification	33%	80%	43%	33%
Illicit trafficking	67%	40%	59%	33%
Loss from military or law enforcement during active use and deployment	17%	20%	14%	33%
State-sponsored diversion	33%	40%	43%	33%
Other	33%	20%	14%	0%
Total respondent Member States in the region	6	5	7	3

Commercial procurement

Non-State armed groups typically rely on purchasing commercial off-the-shelf UAS and UAS components in open markets. This report presents several case studies illustrating this acquisition dynamic (see the section on case study, below). Fourteen respondent States reported this acquisition type, making it the most reported mechanism through which non-State armed groups currently access – or attempt to access – UAS. While not universal, procurement of commercial off-the-shelf UAS was extremely common within the reporting sample – it was reported by three of six respondent States in Africa, three of five States in the Americas, four of seven States in Asia-Pacific and all three respondent States in Europe (fig. 3).

Figure 3
States reporting non-State acquisition of UAS through commercial procurement (n=21)



Commercial off-the-shelf UAS are produced for a wide range of legitimate and valuable purposes such as mapping and surveillance, humanitarian and disaster response, product delivery and transportation, filming, recreational uses, agriculture, forestry and land management. As the range of civilian applications and consumer profiles have expanded, so too have the systems commercially available. Typically, however, commercial off-the-shelf UAS are relatively small, light systems with limits to the range, altitude and speed at which they are able to fly. While some States prohibit the purchase and sale of any commercial UAS, these systems are widely available both online and in retail stores in many countries. As one civil aviation expert from a European State noted at the regional consultations in January 2023:

> You need to think about how you can make it difficult for people to acquire critical parts to use in drone missions. Today you can buy a UAS online or in a store relatively easily, and you can do a lot of damage with this. If you intend to have more effective drones with modern technology, that is more difficult, and you won't find this equipment in the store. For that [export control guidance] we have the Wassenaar Arrangement, which means that whenever one of these companies on the leading edge of drone technologies intend to export something, it is controlled. For me, the Wassenaar Arrangement is one of the key pillars for preventing the acquisition of high-end drone technology by people that shouldn't have access.

As box 2 shows, several multilateral regimes have relevancy to export controls for UAS technology, in particular the Missile Technology Control Regime and the Wassenaar Arrangement. The Wassenaar Arrangement is a voluntary agreement between 42 participating States. It provides guidance and best practices to its members, such as the List of Dual-Use Goods and Technologies, which covers many UAS-related components. States recognized that it is difficult to fully counter the acquisition of UAS components because the versatility of the threat means that – as with developing effective counter-IED strategies, for example – regulators are in a constant "cat and mouse" game with non-State armed groups looking to evade controls and innovate beyond existing restrictions.[31] There are, however, critical component types common to many UAS that are important for export authorities to integrate into national control systems, and for these to be harmonized within and between national export control authorities and customs forces, and clearly communicated with commercial exporters.

Downstream implementation of these regulations requires that the relevant authorities are able to recognize sensitive UAS-relevant components in shipment, and that they conduct careful risk assessments to ensure that materiel is not diverted to unauthorized recipients. In May 2021, for example, the Philippine authorities flagged and halted the export of 117 boxes containing 900 kg of servomotors. The exports declaration indicated that the servomotors would be used for robotics, but the authorities determined that the requested model featured higher specifications than necessary for civilian applications, thus expanding its capability to accommodate multiple programs or software. Following this assessment, the authorities decided to deny the shipment.[32]

Field investigations conducted by CAR have identified multiple occasions in which opaque licensing requirements for multipurpose components that can be used in UAS, such as autopilot units and accelerometers, have facilitated the transfer of materiel for integration into military technology.[33] Communications between exporters and regulatory bodies have shown gaps in understanding and in the implementation of relevant regulations. The same

31. See Chávez and Swed (2023b), who argue that the technology of terrorism is often likened to an arms race between non-State actors and States, and that there is a competitive, asymmetric "technological treadmill" that incentivizes feasible and cost-effective innovations as an organization imperative.
32. This case was the first licence denial of the Philippines export control body following its implementation of the Strategic Trade Management Act; see Fernando (2022).
33. CAR (2021).

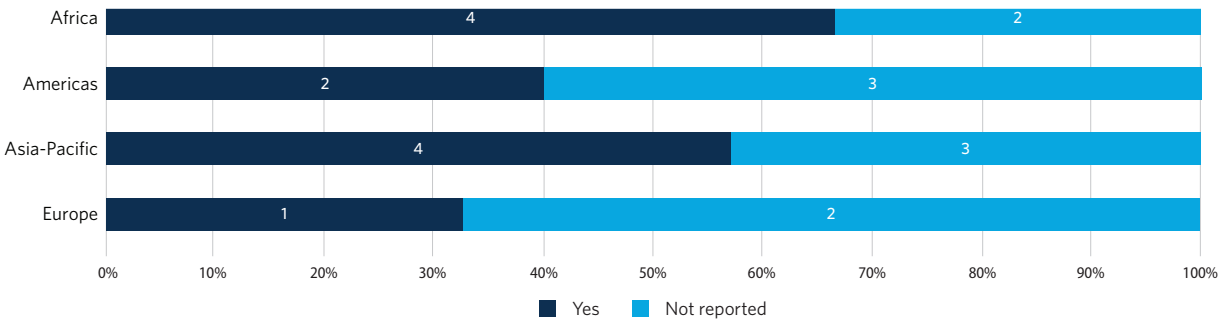
gaps could create conditions for commercial UAS components, or multipurpose components such as engines, to inadvertently fuel non-State acquisition strategies.

Illicit trafficking

The second most common acquisition route is through illicit trafficking, with 52 per cent of respondent States (11 of 21) reporting cross-border movement of material via methods such as postal shipments and smuggling routes. This was reported by four States from Africa, two from the Americas, four from Asia-Pacific and one from Europe (fig. 4).

In an interview conducted for this study in March 2023, a representative of the Government of Yemen identified the illicit smuggling of UAS components as a key acquisition modality pursued by Houthi forces. The respondent shared two examples where components were packaged in wooden containers in an effort to evade metal detectors installed at checkpoints, which were discovered only through manual inspection at the border: the first case was in April 2022, when border security officials uncovered a shipment of 548 wooden propellers; and the second in January 2023, when a seizure uncovered 100 engines each capable of powering a vehicle weighing 95 kg.

Figure 4
States reporting non-State acquisition of UAS through illicit trafficking (n=21)



A related issue of particular concern – which was raised by several Member States – is the transfer of knowledge and expertise between terrorist and non-State groups. A third of respondent States noted that they had observed instances of cooperation between non-State armed groups, including terrorist actors, to acquire UAS through cooperation with other groups, either within national borders or externally, with examples identified in the Middle East, in South America, and in West and Central Africa.[34] This could take the form of attempts to procure development plans and guidance through transnational cooperation; the provision of remote technical or financial assistance; or the movement of key personnel to provide in-person technical support.

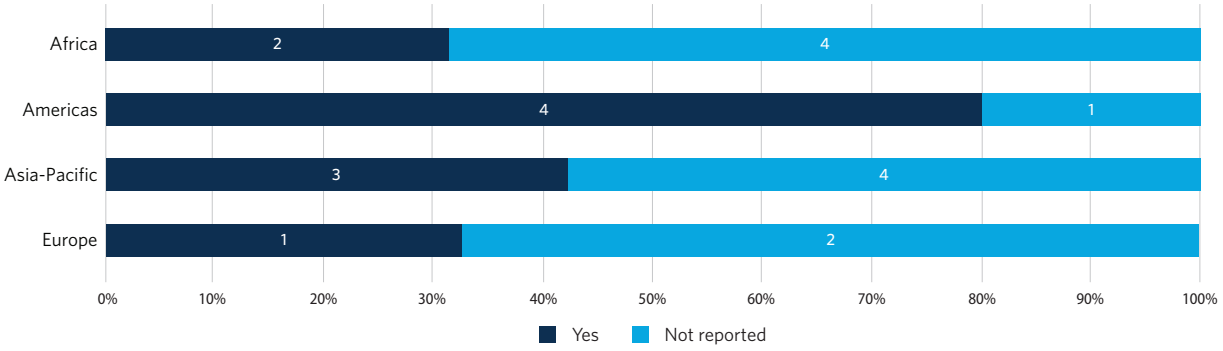
34. A recent quantitative assessment conducted by Chávez and Swed (2023b) identified that "the most statistically and substantively significant predictor of adoption is whether a group is networked with another [violent non-State actor] drone user. This implies that a key mechanism of proliferation among [violent non-State actors] is a technological and doctrinal diffusion through social networks".

The representative of Yemen also reported that the Houthis might already be sharing UAS knowledge and materials with other non-State armed groups in the country, such as Al-Qaida in the Arabian Peninsula, and expressed concern that the proliferation of UAS technical capacity would lead to the "privatization of lethal airspace", with a far more diffuse range of actors, and a more complex airspace, including using UAS in competition with each other. Such knowledge transfer bears parallels with the movement of technical expertise around the construction of IEDs.[35] Although States in South America and the Middle East noted cases where actors used 3D printing to aid in munitions release and critical component manufacture, there is little current evidence to show that this is a major or widespread trend in UAS acquisition. If such a trend becomes more commonplace in the future, it will have significant implications for the further sharing of information and of technical resources between non-State armed groups, including terrorists, as digitizing physical assets and transferring them virtually for 3D printing in a new country will be difficult, if not impossible, to detect and prevent.

Illicit manufacture or modification

The illicit manufacture of UAS – either through the construction of an entire system from scratch, or the substantive modification and enhancement of one already in a group's possession – was the third most reported acquisition approach through which non-State armed groups access UAS. Ten of the 21 respondent States specified this route. This includes two States from Africa, four from the Americas, three from Asia-Pacific and one from Europe (fig. 5).

Figure 5
States reporting non-State acquisition of UAS through illicit manufacture (n=21)



At the regional consultations in January, one State – with extensive national experience of non-State UAS attacks – explained how actors increasingly sought to manufacture their own capabilities in order to develop systems that were capable of launching cross-border attacks. Describing one recent attack, it stated that "none of the parts were manufactured to be part of a UAS, not even a 3D-printed part. They were all made of wood, and the engine came from a lawnmower. It is the hardest part, to follow and trace the parts used to create UAS. For more than two or three years, we don't see any UAS which are manufactured in a factory".

35. As noted in the "Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017)", preventing knowledge transfer entirely may prove impossible, but in the past, legislation prohibiting the possession of IED-related technical knowledge has proved effective in the prosecution of IED makers.

One national civil aviation authority in Europe provided information on an innovative approach to identify specific technological choke points in UAS development. It described a controlled experiment whereby its team attempted to purchase UAS components from open, online sources and assemble their own large UAV, with the capacity to carry a payload of approximately 5 kg. Through this approach, the authority determined that the electric engine constituted the single most important component in UAS development. The authority highlighted that alternative power sources, such as combustion engines, require a much higher level of financial and technical resources to integrate into a purpose-built system, and "so the easiest way [to power a purpose-built UAV] is through electric engines, and these can be obtained in almost any product. You can buy components, software, and you can assemble it; but the electric engine is the fundamental piece and the most important thing to control".

Outlier approaches

The least reported acquisition types by respondent Member States related to the loss or diversion of UAS from authorized custodians. This encompasses losses both "static" (i.e. theft from private or national holdings) and "dynamic" (i.e. abandonment or capture from active deployment). States reporting the acquisition of UAS material through this mechanism are also typically experiencing active violent conflict or insurgencies. This has been raised by analysts as a concern in the past, with several examples to suggest that terrorist and other non-State groups may have sought to reverse-engineer their own systems from downed military-operated UAVs, including in Afghanistan, the Syrian Arab Republic and Türkiye.[36]

While theft of military-grade UAS from storage facilities managed by national security forces may be a rare occurrence at the moment, there is a possibility that this may become a growing pathway to acquisition in the future, especially with reference to civilian-held UAS. The Stolen Drone register[37] is a public database managed by an Australian-based company called DroneSec. It is a public register for self-reporting lost, missing or stolen UAS to enable law enforcement or new prospective buyers to detect stolen UAVs internationally. A search on the register on 3 May 2023 revealed hundreds of UAVs reported stolen by civilian operators in at least 48 countries and territories.[38] Given the relative complexity and scarce availability of UAS, in relation to conventional weapons, it may not be surprising that this acquisition type is not common among Member States. This acquisition type, however, represents an established mechanism through which non-State armed groups consistently access other military material, including conventional weapons, ammunition, and materiel used to produce IEDs. As UAS in general are more frequently deployed by Member States and other lawful users, this may become a more prevalent acquisition type in future research.

36. Chávez and Swed (2020), p. 31.

37. Available at https://stolendrone.info/home.

38. Australia, Austria, Bangladesh, Belgium, Bolivia (Plurinational State of), Bosnia and Herzegovina, Brazil, Canada, China, Colombia, Costa Rica, Croatia, Czechia, Denmark, France, Georgia, Germany, Greece, Hong Kong, India, Indonesia, Iran (Islamic Republic of), Ireland, Italy, Kenya, Malaysia, Maldives, Mexico, Montenegro, Netherlands (Kingdom of the), Norway, Pakistan, Panama, Philippines, Portugal, Romania, Russian Federation, Slovenia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Thailand, Türkiye, United Kingdom of Great Britain and Northern Ireland, United States of America, Uzbekistan.

In the sample of Member States assessed in this study, relatively few reported observing evidence of State support to non-State armed groups as a means to UAS acquisition. Eight of the 21 respondent Member States reported efforts by non-State armed groups to acquire UAS technology through State-sponsored diversion – the process through which a State backs a direct supply of UAS, components or technology to a non-State armed group. This included two States in Africa, two in the Americas, three in Asia-Pacific and one in Europe. Only one respondent State provided information to support its observations (see box 5). At the regional consultations, several Member States expressed the view that an important measure to restrict non-State access to UAS was for the international community to uphold and promulgate global norms prohibiting the provision of UAS technology to non-State armed groups.

BOX 4: EXAMPLES OF NATIONAL PRACTICE TO COUNTER UAS ACQUISITION BY NON-STATE ARMED GROUPS

UNOCT and CAR invited States to provide examples of measures taken to prevent non-State actors from acquiring UAS. States affirmed the existence of various precautionary measures, implemented at the national level, to prevent such acquisition. For example, of the five States that reported having UAS or UAS-component manufacturers, two reported that there was a licensing system in place in the country. Ten of the 21 respondent States reported that they required commercial retailers of UAS to keep records of sales by serial number. Table 6 provides illustrative examples of national policies or operational efforts implemented to prevent the non-State acquisition of UAS.

Table 6
Examples of State practice in relation to UAS acquisition

Example measure	Measure type	Relevant acquisition type(s)
"Precautionary measures implemented by law enforcement such as custom, police and military at the border entry."	Border control	Illicit trafficking; commercial procurement
"Strict vigilance on borders by border security agency and the Police."	Border control	Illicit trafficking; commercial procurement
"Facilities housing such equipment are often protected and their operations are usually classified."	Stockpile management	Diversion from legitimate state or private custodians
"[Introduction of a] law that regulates the use and operations of Remotely Piloted Aircraft Systems (RPAS)."	National legislation	All
"The transaction of UAS are regulated and controlled in the public area. The security forces are briefed to take action against any unauthorized UAS."	Regulation of UAS sales	Commercial procurement
"State drones are protected or secured as usual by the state actors."	Stockpile management	Diversion from legitimate state or private custodians
"In October of 2018, the official authorities in my country prepared a list that includes all the materials that go into manufacturing and equipping drones and distributed them to all sea and land ports and to the military and security units for protecting and monitoring land borders and coasts to prevent the entry of these pieces and materials into the country …"	Border control and training	Illicit trafficking; commercial procurement; State-sponsored diversion

Member State priority concerns

At the regional consultations, Member States identified several trends relating to the acquisition of UAS by non-State armed groups. The concerns centred on three key areas:

Preventing proliferation

In line with existing international obligations for States to refrain from providing any form of support to entities or persons involved in terrorist acts, including by eliminating the supply of weapons to terrorists, several Member States expressed the view that norms against the State-sponsored provision of UAS technology to non-State armed groups should be reinforced and upheld, including through international frameworks. The normative and stigmatizing power of collective opposition to State support to non-State groups through the provision of UAS technology was cited as an important "soft-power" tool to maintain this norm. Additionally, Member States spoke in support of the positive deterrent effect of international sanctions to prevent and restrict States, companies and individuals from promoting the proliferation of UAS technology to non-State armed groups.

With future trends in mind, knowledge proliferation – including the acquisition of guides over the Internet to enable domestic manufacturing – was also noted as a way for non-State armed groups to expand their UAS provisions. States noted the need to prevent and disrupt the movement of personnel with expertise in advanced capabilities who could aid in UAS supply and manufacture.

Regulating and monitoring commercial sales

Member States repeatedly emphasized that access to unregulated or loosely controlled commercial technology was a critical driver of UAS acquisition by non-State armed groups. Given the exponential increase in the technological sophistication of commercially manufactured technologies, commercial off-the-shelf UAS may become more capable of achieving similar ends to military grade systems that typically remain outside the reach of most non-State armed groups. At the regional consultations, one State, a major producer of civilian UAVs, discussed its export control regime for this material. The government has introduced mandatory national standards for commercial off-the-shelf UAS, including technical precautions such as geofencing. Each UAS is marked with a "one-machine, one-code" approach, so that each system bears unique identifiable markings to facilitate tracking and tracing.

Several States commented on the need for clear global regulations regarding multipurpose ("dual-use") commercial components that are used in the manufacture of UAS, as well as clarity around how those components might be integrated into UAS. Restricting access to critical components is one way to inhibit the ability of non-State armed groups to acquire and adapt UAS, while another is to disrupt the recruitment of people with expertise in advanced capabilities who may act as influential facilitators to spread UAS knowledge. Commercial entities themselves are key stakeholders in preventing the commercial procurement of UAS by non-State armed groups. Multiple States highlighted the need for close cooperation and

information-sharing between industry and regulatory and law enforcement bodies. Several States noted that providing advanced guidance to the national authorities regarding new product lines or emerging innovations was a key practical measure to ensure that effective countermeasures could be prepared, should new commercial technology fall into the possession of non-State armed groups. Commercial producers and other transfer parties have an even more tangible opportunity to prevent access to UAS by terrorist and other non-State armed groups, through the adoption and implementation of holistic supply chain security measures. Such measures include heightened due diligence exercises for UAS material, including components.

One industry representative, Skydio, described the complex risk assessment process that it would undergo before authorizing purchases of its products. This included the identification of "red flags" during the procurement process (such as an unrealistic urgency, the provision of unclear or conflicting personal information, or excessive and atypical technical demands); partnering with a third-party validation service to vet non-profits; purchasing open-source intelligence tools to search for information about the individual and the company's history of export compliance; and seeking face-to-face meetings with prospective customers or end users where possible.

Countering illicit trafficking

Several States expressed concern – both through the questionnaire and at the regional consultations – regarding border controls and the continuation of illicit trafficking, including the use of UAS to conduct trafficking. Border control and customs are critical intervention points for several of the acquisition types. Eleven Member States reported that they had made seizures of UAS material in the past 10 years: three from Africa, three from the Americas, three from Asia-Pacific and two from Europe. Police and law enforcement were the most cited agency types responsible for seizing this material from non-State groups (11 of 21 States), followed by armed forces (nine States), and customs and border security (seven States). One State also highlighted recoveries made by private security firms, as well as local community security groups. Six States gave details of the circumstances of recovery. These could be categorized into three broad approaches:

- Seizures from criminal actors operating in national territory
- Interceptions at ports of entry
- Interdiction flying over sensitive sites (prisons, patrols).

An interview with a WCO representative conducted in April 2023 revealed that WCO maintained a customs enforcement network and encouraged its member States to report information relating to seizures of illicit goods. National reporting is voluntary and provides WCO with valuable analytical insights into illicit trade flows, as well as national capacity relating to the control of weapons and other strategic goods. The WCO Harmonized System, which provides a structure for the uniform global classification and reporting of goods traded internationally, has recently been updated so that UAVs are given their own specific provisions. Currently, States are not providing information to WCO on seizures of UAS, and the benefit of recent changes to the global classification codes may not be realized until future reporting.

Seven States reported to UNOCT and CAR that they would welcome greater capacity-building for the national authorities responsible for controlling and preventing UAS access, particularly in the form of training and technical capacity-building. Therefore, providing technical resources to those entities in how to recognize, record and react to UAS material – specifically multipurpose components that may be utilized in UAS design and development – may be an especially effective approach for preventing the ability of non-State armed groups from acquiring UAS.

BOX 5: MULTIPLE ACQUISITION PATHWAYS

One Member State in the Middle East, which has been fighting an armed conflict against a non-State armed group for several years, described how it had identified four main pathways through which UAS are accessed. These pathways speak to a number of the acquisition types identified in table 5, and show how multiple types can be active concurrently in a given context.

1. Smuggling UAS components inside wooden commercial containers to evade border controls and enable assembly and development of systems in country **(commercial procurement; illicit manufacture or modification)**
2. Maritime transfers, with components being loaded onto small fishing boats to evade checkpoints **(illicit trafficking; State-sponsored diversion)**
3. International criminal organizations smuggling material overland through the country's long desert border **(illicit trafficking)**
4. Small UAVs being flown into the country directly from offshore vessels **(illicit trafficking; State-sponsored diversion)**

Several non-State armed groups are active in the country, including terrorist groups proscribed by the Security Council. Representatives of Member States highlighted the transfer of UAS knowledge between non-State armed groups as an emergent concern for security forces and stated that there was evidence of collaboration and movement of personnel between groups that may facilitate the transfer of UAS in the future.

Figure 6

The underside of a commercially available quadcopter UAV that had been weaponized by a non-State armed group to drop an IED from an affixed silicone sealant tube (documented by CAR field investigators in February 2017)

III. Case study: acquisition[39]

Commercial procurement[40]

Da'esh forces in Iraq and the Syrian Arab Republic sought to exploit the commercial availability of commercial off-the-shelf UAS to procure small, electrically powered rotary-wing UAVs. Between 2016 and 2019, CAR field investigation teams documented a sample of 28 quadcopter UAVs which Iraqi defence and security forces recovered during operations against Da'esh.

CAR attempted to trace these commercial systems. Investigations showed that procurement of these UAVs was highly geographically dispersed, with retail purchasers based in diverse locations. CAR was able to trace seven quadcopters to independent distributors in the Middle East, Central Asia and South-East Asia.

Investigators traced one quadcopter to a distributor in the Middle East. The distributor stated that it sold the quadcopter to an IT company in Iraq, which was denied by the company. On 5 November 2015, the United States Treasury placed the distributor and its Chief Executive Officer on its list of Specially Designated Nationals, alleging that it had acted as a procurement agent for Hizbullah, purchasing UAS and accessories from companies in multiple companies. The Chief Executive Officer strongly denied having any connection to Hizbullah, and the investigations did not find evidence that the activities alleged by the Treasury were connected to Da'esh UAV procurement.[41]

In another sale traced by investigators, two of the UAVs that CAR documented in Iraq had been sold to a company in the Middle East region in August 2016. The company told CAR that it sold all of its UAVs individually to cash-paying retail customers, but did not maintain records of customers or of serial numbers. Notably, the manufacturer listed the UAVs it shipped directly to the company as "digital cameras" on shipping documentation. Such a categorization may make it more difficult to monitor international shipments of commercial UAS. There is no evidence that the companies involved in this case were in any way complicit in the diversion of these quadcopters to Da'esh, or that they had any advance knowledge of their final end user.

Controlling acquisition

Several intervention points are available to States and commercial actors attempting, in cases such as these, to prevent the diversion of commercial off-the-shelf UAS to non-State armed groups, including terrorists (fig. 7). Before acquisition, the completion of a comprehensive risk assessment prior to initial shipment to distributors would help "red flag" entities that had

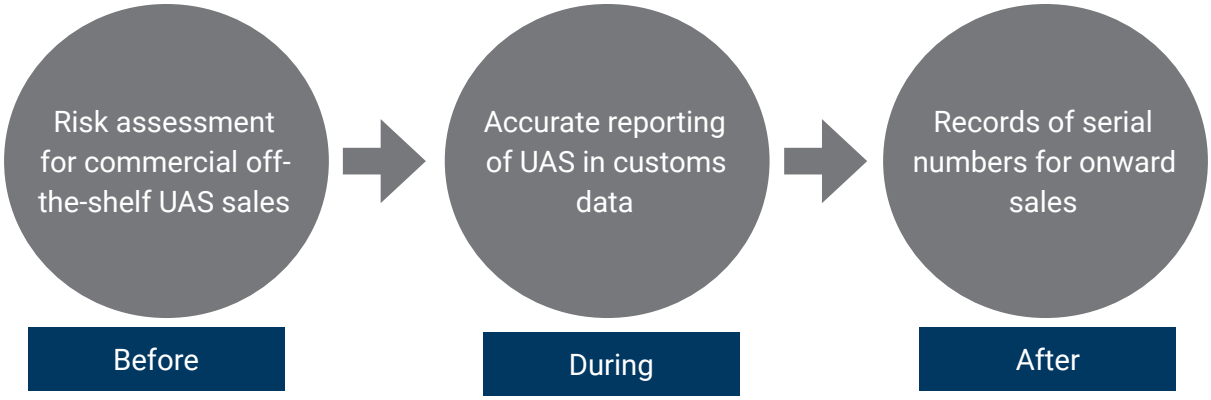
39. The case studies are drawn from field investigations conducted by CAR. Although they illustrate specific examples of acquisition efforts, they are distinctive to specific contexts in which CAR operates, and are not representative of all issues relating to, and arising from, the acquisition of UAS by non-State actors.

40. Information used in this case study is derived from CAR (2020b).

41. US Department of the Treasury (2015).

a record of involvement in problematic onward sales. While the diffuse nature of commercial supply chains means that it is not possible for a manufacturer to verify the final end user of each transfer, there may be downstream cooperation measures that could help to limit the risk of commercial off-the-shelf UAS reaching terrorist actors. These include requiring a commitment from the distributor not to allow transfer of an item to an end user outside the country of sale without permission from the manufacturer or conducting due diligence of customers to verify end-use. During transfer, the accurate reporting of UAS in transfer documentation will greatly enable the ability of customs officials to monitor sales and to track whether goods are being moved out of the country. If distributors and commercial retailers were to keep records of sales of commercial off-the-shelf UAS by serial number, this would greatly increase the ability of investigators to monitor and track customers purchasing UAS that are destined for non-State armed groups, including terrorists.

Figure 7
Intervention points to counter terrorist acquisition of commercial off-the-shelf UAS



Multipurpose components

From 2014 to 2017, acquisition networks acting on behalf of Da'esh forces in Iraq and the Syrian Arab Republic sought to procure a range of items intended for the development of specialized UAS. These included engines, component designs, optical systems and bespoke software.

In December 2014, for example, a company based in a west European Member State purchased a microturbine – a small turbojet engine – from a supplier of turbines and civilian UAVs based in another European Member State. The purchasing company's primary business was the provision of electronic point-of-sales systems for restaurants and retail business and had no apparent connection to UAS.

The company paid €2,400 for the microturbine via bank transfer from its bank account registered in western Europe. However, it subsequently instructed the supplier to dispatch the microturbine to a company address in the Middle East. This was one of several similar purchases of UAV components and counter-surveillance equipment made during this period either by this company based in western Europe or by other related associates. Orders and payments were all made online, often through third-party providers, using accounts registered to representatives of two companies registered in the west European Member State.

The two companies were registered at the same address. One company was registered under fictitious names for its directors and shareholders. Several fictitious employees were created, ostensibly to discuss technical and business questions with suppliers via email. For each order, these fictitious company representatives would either instruct suppliers to send goods directly to the same location or to the same individuals in a town near an area of the Syrian border that, at the time, was under Da'esh territorial control – or would arrange for an employee to collect the goods from the company's address in Europe and then redispatch them to the location near the Syrian border. During the same period, the same companies also made a series of large purchases of precursors used for development of IEDs, such as aluminium paste, which were also shipped to the same location.

Tackling component diversion

Many high-end components for commercial off-the-shelf UAS are already covered in multilateral control regimes such as the voluntary Wassenaar Arrangement. States may view cases like the above as justification to subject these components to enhanced export control measures. Requiring detailed corporate due diligence for these sensitive goods would help to identify risk factors, such as a pronounced mismatch between the purchasing business and the requested goods, or instruction to ship goods to a different country, especially if that is known to be in, or close to, territory held by a non-State armed group. Manufacturers may seek to unliterally implement further precautionary controls. This might include requiring face-to-face meetings with a prospective purchaser, or a prohibition on payments through online third-party applications that make it hard to detect suspicious transactions.

Active trade and end-use monitoring after a sale may help to track choke points in non-State armed group supply chains; commercial entities that act as a critical junction point for multiple shipments of goods. In the case described above, the network sought to procure individual UAS components from multiple diverse companies in different countries. Treated as isolated sales, they may not have appeared suspicious. Taken together, these transactions, alongside purchases of material that could be used in the production of IEDs, would represent a clear red flag to companies and law enforcement working to prevent diversion of UAS and UAS components.

Figure 8
Intervention points to counter terrorist acquisition of multipurpose components

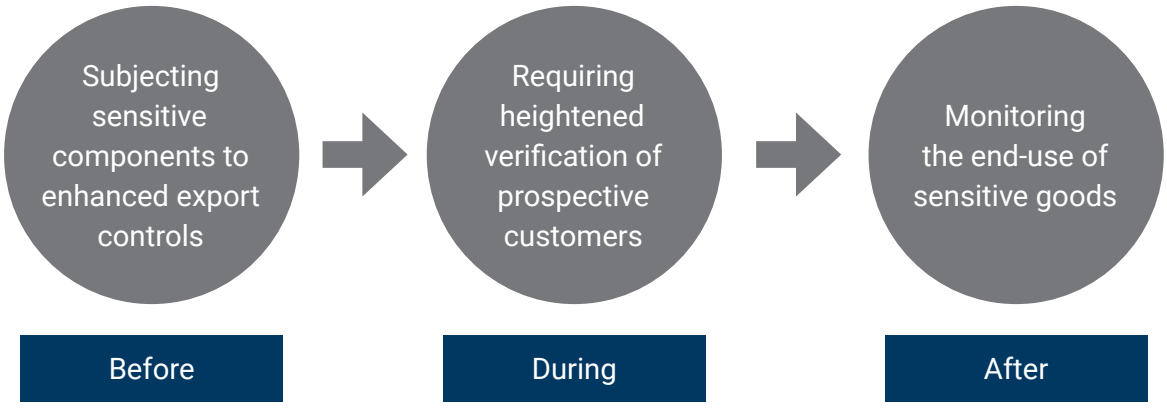


Figure 9

A small projected IED that was developed by a non-State group for multiple roles, including delivery from a commercial off-the-shelf UAV (documented by CAR field investigators in March 2017)

IV. Weaponization

Trends in weaponization

As shown in the previous section, the predominant acquisition trends are for non-State armed groups to acquire UAS through commercial procurement or illicit trafficking. Therefore, the systems that are typically available to non-State armed groups are not – in the main – advanced, powerful, military-grade UAS, with existing weapon capacities. This section focuses on how non-State armed groups are customizing existing systems to make them more lethal. The term "weaponization" refers to a process whereby non-State armed groups, including terrorists and criminal groups, modify UAS already in their possession to increase their capability to carry out attacks.

This term is usually applied solely to modifications that result directly in the arming of a previously unarmed UAS. This report adopts a more expansive interpretation to include other modifications that can be considered potential force multipliers by changing the existing capacities beyond the intent of the manufacturer. For example, the addition of a camera payload is a modification that would increase the capacity of a non-State group to use UAS in its possession to carry out more precise attacks. Adding a camera may therefore be regarded as a step towards later weaponization. Monitoring steps taken that may be part of a non-State armed group's engineering pathway to develop fully weaponized UAS could provide Member States with early intervention points to prevent the development of UAS with attack capabilities. How a non-State armed group seeks to weaponize UAS in its possession may give great insight into that group's motives, available resources, level of organization and operational objective. It would therefore be highly instructive for future research to seek to establish the scale of observed weaponization efforts in each respondent country, where appropriate. Understanding whether an identified case of weaponization represents an isolated outlier experiment – or is reflective of efforts to establish a standardized and semi-industrialized process – would be significant to trend analysis and evaluations of the level and nature of the UAS threat in specific contexts. It would also be important to inform the development of relevant national action plans to counter this threat, and to determine capacity needs at the national level. As one representative from a European Member State, a counter-terrorism analyst, noted at the regional consultations in January 2023:

> The terrorist groups that we are most concerned about are those that have dedicated programmes. If they have dedicated resources, expertise, and funding, and if they have access to facilitation networks so that they can gain access to components or commercial drones, those are the most dangerous groups.

Da'esh forces in Iraq and the Syrian Arab Republic represent one of the most advanced examples of organized weaponization by a non-State armed group. A study conducted in 2017 by the International Center for the Study of Violent Extremism identified that the group established a

complex UAS development programme that included a dedicated training centre; a specialist, centralized team of technicians and engineers to modify commercial UAVs to drop IEDs; and a storage site to manage distribution requests from front-line terrorists. Da'esh embarked on a series of attempted innovations to weaponize commercial UAS in its possession, including the inclusion of solar panels to increase their operational life, and the addition of multiple small IEDs.[42]

A total of 11 of the 21 respondent Member States (52 per cent) reported observing one of the five mechanisms described in table 7. This includes four of the six respondent States from Africa, two of five States from the Americas, four of the six States from Asia, and one of the three States from Europe. Weaponization as a phenomenon was not distinct to any particular region – and not restricted to countries experiencing active armed conflict – although it was reported more by the respondent States from Africa and Asia-Pacific.

Table 7
Types of attempted or actual weaponization of commercial UAS reported by Member States

Mechanism	Description	Breakdown	Total
Camera payload	Devices that can record audio, still images or video footage.	Africa (3), Americas (2), Asia-Pacific (3)	8
Conventional ammunition or IEDs	Modification to include an explosive payload may take different forms, including the use of conventional ammunition like mortars, rockets, missiles or grenades, or the addition of commercial or home-made explosives to create an airborne IED.	Africa (2), Americas (1), Asia-Pacific (3)	6
Dispersal or spraying	Non-State armed groups may seek to create their own weaponized "spraying UAVs" through the addition of containers of chemical or biological agents that, combined with ventilation fans or aerosols, release a toxic substance. These dispersal mechanisms may be improvised or purchased/taken from commercial off-the-shelf agricultural UAS.	Africa (2), Asia-Pacific (3)	5
Release mechanism	A release mechanism may be a purchasable UAS component that is added to a compatible UAS. It may also be a fabricated device, developed through local manufacture or 3D printing. In both cases, the release mechanism is used to release a payload on a target below.	Africa (2), Americas (2), Asia-Pacific (2), Europe (1)	7
Other*	Weaponization types not addressed by the above descriptions. States were invited to provide details about how non-State armed groups operating in their State weaponized – or attempted to weaponize – UAS.	Africa (1)	1

* No details were provided by the respondent State.

Figure 10
Percentage of respondent States that observed different weaponization types (n=21)

Weaponization type	Africa	Americas	Asia-Pacific	Europe
Camera payload	50%	60%	29%	0%
Conventional munitions/IEDs	33%	20%	29%	0%
Dispersal or spraying mechanism	33%	0%	29%	0%
Release mechanism	33%	40%	29%	33%
Other	17%	0%	0%	0%
Total respondent States	6	5	7	3

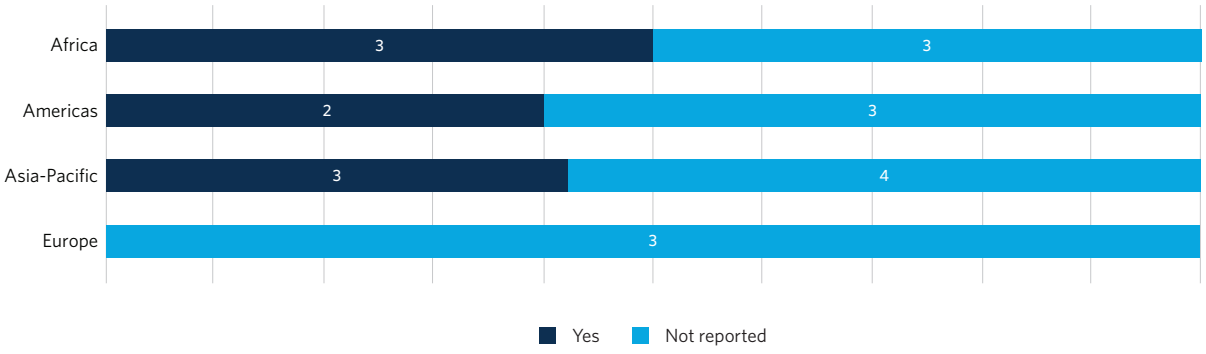
42. Almohammad and Speckhard (2017).

Facilitators (camera payloads, release mechanisms)

The two most common modification types reported by respondent Member States were both facilitators of weaponization, rather than forms of weaponization themselves: the addition of a camera payload, and the application of a release mechanism. Neither of the two mechanisms result in a weaponized UAS, but may signal attempts by a non-State group to advance their attack capabilities.

Camera payloads can include 4K high-definition recreational video cameras designed for performance in all terrains and weather. Some UAVs with this capacity have a near real-time transmission capability, while older technologies will have data that can be extracted on return to operator. Eight States reported observing this form of UAS modification: three from Africa, two from the Americas and three from Asia-Pacific (fig. 11). The addition of a camera would not result in a UAS being classified as weaponized, but the pursuit of this modification by non-State armed groups may be considered to be a critical "facilitator" to the capabilities of non-State armed groups to carry out hostile acts, whether directly (i.e. enabling UAS to conduct surveillance of Member State personnel and infrastructure) or indirectly (i.e. enabling human operators to maintain a visual feed to direct munitions delivery more accurately). It may also include the replacement of original cameras with higher capability devices such as thermal imaging systems that would enable operations in dark conditions.[43] UAVs with in-built, high-definition cameras are becoming more common across many commercial models, and therefore this trend could diminish in the future.

Figure 11
States reporting modification of UAS with a camera payload



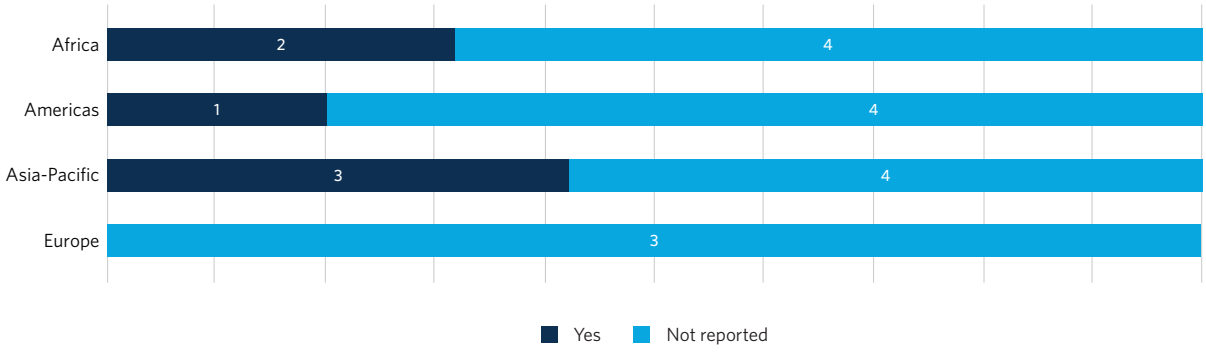
Seven States reported observing attempts to integrate a release mechanism into a UAS. The addition of such a mechanism may be regarded as a concrete step towards weaponization as it would enable the UAS to drop a payload to a target according to the needs of the operator. This may relate to effectively arming a UAS with explosives (see below), or another form of payload such as dropping propaganda material in the form of leaflets, for example. Two Member States in Africa, two in the Americas, two in Asia-Pacific and one in Europe reported observing this modification by non-State armed groups in their country. Five of these States also reported weaponization through the addition of explosives, but two (one in the Americas and one in Europe) reported only the inclusion of a release mechanism.

43. For a case study illustrating this dynamic, see Rogers (2019), which describes how a Danish citizen purchased 20 thermal imaging cameras from a hobbyist shop to be smuggled into the Syrian Arab Republic for integration into UAVs developed by Da'esh technicians.

Conventional ammunition or IEDs

Six respondent States highlighted the attempted or actual addition of an explosive payload, either in the form of IEDs or conventional munitions (fig. 12). This mode of weaponization is not solely observed in countries affected by conflict or active insurgencies. For example, at the regional consultations, one respondent State from the Americas stated that in 2022 security forces had, for the first time, observed UAVs modified to carry explosive payloads. This was also observed by other Member States from the Americas. In Mexico, the Jalisco New Generation Cartel (CJNG) – an organized criminal group – has deployed UAS to gather intelligence on Mexican law enforcement. However, these UAS have also been used to highlight targets for attack and to conduct kinetic strikes against law enforcement personnel. CJNG has been known to use weaponized UAS in a rudimentary yet effective manner, for example by taping plastic explosives and containers filled with ball bearings that can be detonated by remote control.[44] In 2017, police in Guanajuato, central Mexico, seized a commercial off-the-shelf quadcopter armed with an IED, reported as a "home-made grenade". By 2021, the group's capacity to weaponize systems in its possession had evolved to the extent that it was reportedly able to conduct attacks with multiple systems. In one incident, two UAVs were used to drop explosives on security forces, injuring two officers as they cleared roads in Michoacán province that the group had blocked earlier.[45]

Figure 12
States reporting weaponization of UAS with an explosive payload



Non-State armed groups, including terrorist groups, may use or modify items of conventional ammunition to act as explosive payload that can be dropped or even launched by a customized commercial UAS (see box 6). Mortars, rockets and grenades are the most common forms of conventional ammunition that could be released, or launched, from a UAV. These munitions are of a suitable size and weight for commercial systems to carry effectively.[46] They may also be more prevalent in the holdings of non-State groups than larger systems that are less frequently diverted, such as guided munitions. Non-State armed groups have, in some cases, reduced the weight of these payloads by replacing metal components with plastic or 3D-printed elements. The UAV can also release an IED or be converted into an airborne IED itself – mimicking the functioning of one-way attack UAVs that are piloted directly into

44. BBC News (2021).
45. Hambling (2021).
46. Commercial UAS typically fall under the Class I NATO classification (i.e. with a maximum take-off weight of 150 kg). Classifications taken from United Kingdom, Ministry of Defence (2017).

a target. These expendable, single-use aircraft are sometimes likened to guided munitions.[47] Non-State armed groups may seek to weaponize a commercial off-the-shelf UAS by packing it with an explosive payload – sometimes at the expense of a camera – and fitting it with a remote, impact or proximity detonation device.

BOX 6: RAPID EVOLUTION OF UAS

At the regional consultations held for this study, one State shared its experience with countering non-State use of UAS since 2015, and how the nature of the threat has evolved rapidly. The example presented below was shared by a Member State under the Chatham House rule, and therefore cannot be attributed in this report.

Stage 1

The first non-State UAS observed were exclusively unmodified commercial systems, used in observation and reconnaissance activities. These systems were radio-controlled and relatively easy for security forces to disrupt.

Stage 2

Within a short space of time, non-State armed groups began to heavily modify these systems, adding release mechanisms, improving the antenna systems and removing original cameras with lighter ones so that the payload space could be used to add conventional munitions such as mortars.

Stage 3

Non-State armed groups began to deploy fixed-wing UAS, which were able to fly at higher altitudes and over greater distances. These were much harder to detect. These UAS also had a fallback control system and could be navigated using GPS waypoints.

Stage 4

From 2018 onwards, non-State armed groups began to remove the camera and radio control receiver in order to load a greater quantity of explosives. Without the camera or means of in-flight data transmission, these UAS began to mimic the functions of guided munitions. Technicians with the non-State armed group added laser sensors, custom electronics and a proximity fuse. These systems could fly over distances greater than 50 km and were able to travel using in-built sensors meaning that they were not dependent on radio control or GPS connections.

Stage 5

In 2021, the State first observed the use of UAS containing internal combustion engines. These engines have far greater capacity than earlier power sources. These UAS can fly up to 300 km and can carry payloads weighing as much as 25 kg. They also have a third communication fallback: in addition to radio control and GPS, these vehicles are fitted with a full band global navigation satellite system (GNSS) receiver.

47. One-way attack UAS can include "loitering munitions" with the ability to orbit above a location until a target is identified either by the operator or the automated sensors aboard the aircraft. See Gettinger (2023).

Outlier approaches

Dispersal or spraying mechanisms

Commercial UAVs with spraying systems have been developed to support, for example, large-scale agricultural activities. Non-State armed groups, including terrorist groups, may seek to create their own weaponized "spraying UAVs" through the addition of containers of liquid chemicals or biological agents that, combined with ventilation fans or aerosols, release the toxic substance. Five Member States reported that this mode of modification had been attempted or actualized in their countries by non-State armed groups (two States from Africa and three from Asia-Pacific). While the purpose of the addition of this mechanism was not reported for this study, one concerning possibility is the attempted dispersal of a chemical or biological agent. This was raised as a potential deployment concern by several States. One State in the Asia-Pacific region stated that it had observed terrorist actors in its national territory attempting to use UAS to attack cities and neighbouring countries with chemical weapons.

There are concerns about non-State armed groups using UAS to deliver chemical, biological, radiological or nuclear (CBRN) agents. Security Council resolution 1540 (2004) requires Member States to adopt and enforce effective measures to establish domestic controls to prevent the proliferation of CBRN and their means of delivery. A 2021 study conducted by the UNOCT United Nations Counter-Terrorism Centre and UNICRI identified three broad possible concerns relating to non-State use of UAS: use of UAS to release CBRN materials, for example during a major event; use of UAS to attack and sabotage CBRN facilities; and use of "swarms" to carry CBRN materials.[48] The use of UAS to deliver CBRN is therefore an extremely serious and significant threat, but one that empirical evidence suggests has, so far, not been something that non-State armed groups have proved capable of weaponizing.[49] As noted by one State expert at the regional consultations, this may in part be a result of the relative complexity of creating improvised chemical or biological payloads: "We've seen terrorist groups experimenting in this space, but I think probably the downsides of using chemical weapons, not from an ethical point of view but a practical one, may be enough to dissuade its use. If you want to kill people in a defined area, you might be better off with explosives … my understanding is that there is a lot of science involved, a lot of experimentation". While this is identified in the present research as a relative outlier, there have been rare cases of non-State armed groups attempting to deploy UAS involving CBRN elements, such as in Japan in 2015, when an environmental protester flew a UAV carrying a container of radioactive sand onto the roof of Prime Minister Abe (see table 1).

48. UNOCT United Nations Counter-Terrorism Centre and UNICRI (2021a).
49. Ibid.

Other payloads

Although one State selected "Other" in this reporting field, no further information was provided. Other possible types of UAS weaponization include the introduction of a "communications payload" (i.e. a 3G, 4G or 5G transmitter capable of transmitting mass messages to affect the morale of ground-fighting troops, for example), or the addition of a mounted firearm to a UAV. Such systems could potentially be modified to intercept or interfere with electromagnetic signals.

Member State priority concerns

Preventing direct attacks

The most prominently expressed priority was the modes of modification that would enable direct kinetic attacks using UAS. Six Member States responded to the questionnaire identifying the use of "armed UAS with an IED" as an emerging development that is of the greatest concern (two in Africa, three in the Americas and one in Asia-Pacific). In an interview on 20 October 2022, United Nations officials noted that – while to date there had been no lethal attacks on peacekeeping operations using UAS, and despite investment in deterrence and mitigation measures by the United Nations – it was "only a matter of time before we see lethal use". In 2022, for example, the United Nations received unconfirmed reports that national security forces, in a country where United Nations peacekeepers were operative, had shot down a commercial off-the-shelf UAS fitted with an IED. The non-State use of UAS is the highest designated threat for at least one peacekeeping mission in Africa, and the threat of direct attack, including with explosives, is one that is growing in several operational contexts. This speaks to the critical importance of limiting conventional ammunition diversion, and ensuring strict controls over the transfer and security of precursor materials that can be used to create IEDs.[50]

Responding to the emergence of artificial intelligence

The potential for non-State armed groups to harness developments in artificial intelligence (AI) was highlighted by Member States in Europe, Africa and the Americas as a point of concern.[51] This is advanced technology that is in relatively early development in military-grade UAS, and Member States did not report observing this technology in weaponized or modified UAS in the possession of non-State armed groups currently.[52] UAS are, however, quickly becoming test vehicles for the application of increased AI automation in society. As more advanced AI

50. Unsecured ammunition and military explosives provide non-State armed groups with easy options for the development of IEDs, and repurposing for use by UAS, and there is a strong case to be made for prioritizing enhanced ammunition controls as a critical element of global counter-terrorism efforts. See CAR (2018).

51. For more information on the malicious use of AI for terrorist purposes, see UNOCT United Nations Counter-Terrorism Centre and UNICRI (2021b).

52. A 2023 survey conducted by researchers at Royal Holloway, University of London, and the Center for War Studies, at the University of Southern Denmark, identified 24 military-grade loitering munition UAS that were advertised as possessing autonomous and automated features, either related to targeting or flight capabilities. These systems were either in the possession of State militaries or in development and were not commercially available. See Watts and Bode (2023).

and autonomous systems become available on commercial markets, these may eventually be acquired by terrorists and other non-State armed groups.[53] Weaponization of commercial off-the-shelf UAS with this technology would create improvised autonomous weapons systems capable of selecting, engaging and striking targets in a completely autonomous manner.

Reacting to fast-evolving technological advances

Member States further raised concerns regarding the rapid evolution in technological advances that non-State armed groups could potentially make in the near future. These go beyond the addition of a weapon capability and include any customizing of existing products that enable it to evade existing countermeasures, conduct operations more "effectively" or otherwise increase the threat capacity of UAS. An overview of the various types of technological advances and their possible integration, carried out by UNIDIR researchers, has shown that these indeed would aim to improve the existing capabilities of UAS.[54] States also identified modifications intended to expand flight capabilities through more powerful commercial engines, fixed-wing advances or innovative power sources such as solar charging, as changes that could allow weaponized UAS to fly higher, making them harder to be detected or destroyed.

Several Member States highlighted concerns that increasing numbers of UAS could be used in en masse deployment, rudimentary swarm or true swarm attacks.[55] The deployment of large numbers of low-cost UAS to overwhelm countermeasures may not be a prohibitively complex or expensive technology for non-State armed groups to adapt (see the section on deployment for more on swarm attacks). States also documented concerns that UAS will become harder, if not impossible, to detect and destroy. This could be through the adoption of more effective tactics (such as low-altitude flight and slower-speed designed to evade existing radar) or the procurement of more advanced technologies (such as multi-frequency navigation controls, or new designs such as mini or micro UAS to elude the current generation of counter-UAS). Finally, States also signalled the spread of "5G remote piloting" as a worry that will facilitate ever more resilient, accurate and longer-range UAS flight by a growing number of groups.

One specific concern identified at the regional consultations was that advances in open-source and online abilities could mean that non-State armed groups grow more capable in unlocking manufacturer fail-safes. These "breaker apps" could negate preventive restrictions installed at the point of manufacture of a commercial off-the-shelf UAS, such as geofencing or anti-collision systems. In fact, a degrading of counter-UAS effectiveness was a point of concern, with several Member States expressing that rapid changes in technology may inhibit the effectiveness of counter-UAS technology options.

53. Rogers and Kunertova (2022).

54. Grand-Clément and Bajon (2022a).

55. Military analysts have noted that the development of 5G will "become an absolute game-changer for small-to-medium-sized [UAS] … swarming technology is likely to evolve further [and] it will be possible to control swarms by a single operator and in real time as a result of 5G networks"; see Mackenzie and Kanellos (2021).

Multiple respondents highlighted that their national experience showed that there was no technical silver bullet to the growing problem of UAS weaponization. States identified the need for a holistic and interlocking set of policy, regulatory and technical countermeasures to counter the acquisition and weaponization of UAS. Box 7 includes some examples of legislative and operational measures identified by States during research for this study which relate to UAS weaponization by non-State armed groups, including terrorists.

BOX 7: EXAMPLES OF NATIONAL PRACTICE TO COUNTER UAS WEAPONIZATION BY NON-STATE ARMED GROUPS

The UNOCT and CAR questionnaire issued to Member States invited them to provide examples of measures taken to prevent non-State actors from weaponizing UAS. Of the 21 respondent States, 17 said that they had some form of legislation to prohibit the modification of commercial and recreational UAS. Table 8 provides illustrative examples of national policies implemented to prevent the non-State weaponization of UAS.

Table 8
Examples of State practice relating to weaponization of UAS

Example measure	Measure type
"We have specific legislation that controls private production and modification [of] UAS"	National legislation
"The private use of civilian UAS is controlled … and may not be modified for the purpose other [than] the one signed for. For example … an UAS designed for camera cannot be modified for another task, like for military purpose or transportation."	National legislation
"According to the implementing rules and delegated rules of the European [Union] Aviation Safety Agency (EASA)."	International policy/ guidance
"The UN follows ICAO regulations which do not allow modifications of commercial UAS by non-authorized entities."	International policy/ guidance
"The official authorities … only allowed very small planes that are used for photography only and in areas under their control only (the flight height does not exceed more than 300 meter above the ground, its load does not exceed 2 [kg], and it does not have a loading platform."	Restrictions on UAS
"The total mass of the civilian drone must not exceed 800 g."	Restrictions on UAS

Figure 13

A modified IED recovered from a non-State armed group. It was intended for delivery from a commercially available UAV (documented by CAR field investigators in March 2017)

V. Case study: weaponization[56]

Weaponizing with conventional ammunition

On 21 February 2016, a CAR field investigation team inspected a building in Ramadi, Iraq, that had recently been abandoned by Da'esh forces. The building had been used as a production facility, at which Da'esh had been attempting to build UAVs (a UAV workshop). Photographic evidence from the workshop shows attempts to manufacture large UAVs from scratch, with a range of component parts under construction, including fuselages and wings, as well as avionics such as camera controllers and gyro sensors, which are used to control an aircraft in flight.

The CAR investigation team also discovered in the workshop an incomplete 9K32M Strela-2M (SA-7b) man-portable air defence system (MANPADS) and the disassembled components of a 9M32M MANPADS missile – notably the warhead section and the missile's steering unit. The co-discovery of UAV construction alongside attempts to repurpose missile components plausibly suggests attempts by Da'esh forces to develop some form of weaponized UAV.[57]

CAR also documented bulk supplies of resistors, transistors and signal relays, which were packaged and marked to indicate production in East Asia. Markings on the relays showed that they had been manufactured in 2013 and 2014. The signal relays were identical to others that CAR had consistently documented in radio-controlled IEDs manufactured by Da'esh.[58]

Adding payload-dropping capabilities

CAR field investigators in Iraq documented evidence of Da'esh modifications to small, commercially available quadcopter UAVs. These UAVs were customized so that they could release a small explosive payload.

CAR documentation shows how Da'esh technicians affixed an empty sealant tube to the underside of the craft. The tube housed a small IED and held it stable to prevent it from swinging during flight. The IED could be released remotely when the UAV was directly above an intended target. A metal wire loop fitted to the base of the IED was held by a rod attached to a servomotor. The operator of the quadcopter could then transmit a radio signal to a custom switching circuit that actuated the servomotor and retracted the rod, causing the IED to fall to its target.[59]

56. The case studies are drawn from field investigations conducted by CAR. Although they illustrate specific examples of weaponization and modification efforts, they are distinctive to specific contexts in which CAR operates, and are not representative of all issues relating to, and arising from, the weaponization of UAS by non-State armed groups.
57. CAR (2016b).
58. CAR (2016a).
59. CAR (2017b).

This example illustrates several of the challenges associated with countering UAS weaponization. The acquisition of these materials was highly opportunistic, including items procured locally and informally. The release mechanism, although innovative, was both cheap and easy to replicate.[60]

Modifying to increase power and range

Da'esh technicians have sought to develop larger, faster UAVs than those available on commercial markets. These plans would be powered by pulsejet engines, a type of acoustic jet engine that is relatively inexpensive and technically unsophisticated, but have been used by amateur enthusiasts to power model aircraft capable of speeds greater than 250 km/h.

In August 2015, an individual posing under a pseudonym made an online purchase of plans for a large pulsejet engine capable of approximately 50 lbs of thrust. The individual – the same person involved in the purchases of UAS components – placed the order with a North American company, emailing to ask whether the engine would be capable of powering a 40-kg model aeroplane. Two years later, in September 2017, an unexploded ordnance and IED clearance operation discovered a fully constructed pulsejet engine at the site of a former Da'esh weapons production facility in Mosul, Iraq. The engine measured more than 2 m in length and featured a machine air-intake head and a motorbike spark plug for ignition. It also featured several differences to the plans purchased online from the North American company, including a "daisy-valve" arrangement for the intake, suggesting that Da'esh had successfully obtained jet engine expertise from other unidentified sources.[61]

Preventing weaponization of UAS

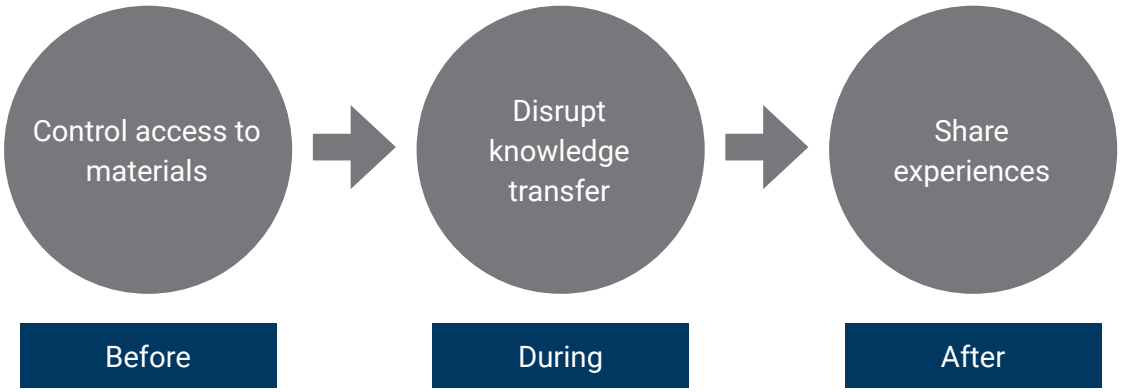
In order to successfully weaponize a commercial off-the-shelf or custom UAS, non-State armed groups require three things:

- Materials
- Tools
- Knowledge

While preventing weaponization in such cases may be extremely challenging, each of the three areas listed above constitute preconditions for modification. As such, they provide States with prospective intervention points to disrupt and inhibit efforts from non-State armed groups to create weaponized UAS (fig. 14). Blocking access to materiel is one key intervention point for States, namely by implementing stringent and holistic supply chain controls to prevent diversion of conventional ammunition or precursor materials used in IED production. Another is to disrupt the transfer of knowledge between non-State groups, which may take the form of sharing alerts between intelligence about individuals with expertise in UAS weaponization. Finally, States identified the value of confidential regional or international forums where information can be shared at an operational level relating to new and emerging weaponization trends.

60. Rassler (2018).
61. CAR (2020b).

Figure 14
Intervention points to counter terrorist weaponization of UAS



BOX 8: EXPLOITATION OF UAS

UNOCT and CAR asked Member States to identify and clarify their capacity to recover UAS and conduct effective forensic analysis. Such capacities enable Member States to investigate the users and supply sources of UAS recovered in their countries and conduct appropriate judicial and law enforcement activities, in accordance with national law.

- Thirteen States reported the capacity to recover, analyse and preserve **physical** evidence of UAS and UAS components.
- Seven States reported the capacity to recover, analyse and preserve **biometric** evidence of UAS and UAS components.
- Eleven States reported the capacity to recover, analyse and preserve **digital** evidence of UAS and UAS components.

Only six States reported effective capacities in each of the three areas: one from Africa, one from the Americas, two from Asia-Pacific and two from Europe. Five States reported the absence of any of the three evidence-gathering capacities.

Five States – one in the Americas, three in Asia-Pacific and one in Europe – reported examples of successful prosecutions of individuals who had unlawfully acquired, weaponized or deployed UAS for use in criminal or terrorist incidents. Two of these States clarified that the prosecutions related to attempts to bring goods into prison. Another explained that "authorities … have transferred the people they arrested while smuggling drones and their parts and equipment … to the judicial authorities for investigation and imposing deterrent penalties on them".

Only two of the 21 States stated that the national authorities had presented UAS digital forensics in court. Neither State reported examples of successful prosecutions in the previous question.

Of the 21 respondent States, six – two in Africa, two in the Americas, one in Asia-Pacific and one in Europe – reported having the appropriate facilities (a laboratory or similar) to convene a UAS digital forensics procedure with a seized, intercepted, captured or otherwise recovered UAS. Another four stated that developing such facilities was of interest but not currently available.

Figure 15
A combat UAV, captured from a non-State armed group (documented by CAR field investigators in February 2017)

VI. Deployment

Trends in deployment

Deployment refers to the operational objectives and targets in which non-State armed groups, including terrorists, seek to use UAS. Prior to the development of UAS, State forces had unchallenged control over airspace – particularly in higher altitudes – and an effective monopoly over the use of aerial force. The introduction of UAS undermines this control and introduces new offensive and defensive capabilities to non-State armed groups.[62] Although commercial UAS may now represent a low-cost route to aerial power – relative to the recent past – they still represent high-value assets to non-State armed groups, including terrorist groups.

Representatives of 11 of the 21 Member States indicated that they had experienced attacks, disruption or other incidents involving the use of UAS by non-State armed groups. Respondents stating that they had experienced incidents were not centralized in any one region (two in Africa, four in the Americas, three in Asia-Pacific and two in Europe), nor were they solely countries affected by active armed conflict.

As noted in the Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems, the possible misuses of UAS by terrorists are extensive and varied and can be directed against an equally wide variety of targets.[63] Deployment modes can be as varied as the need of the operator and the capabilities of the system. At the consultations, multiple States noted that non-State armed groups sought to learn deployment methods from each other, and that the ability of UAS to record its own deployment presents a showcase for different, and novel, use cases that speed up learning and "copycat" approaches between groups.

In the questionnaire, UNOCT and CAR invited Member States to identify ways in which UAS had been deployed, or had attempted to be deployed, by non-State armed groups. UNOCT and CAR drew on the Berlin Memorandum and other expert sources to derive a non-exhaustive list of 11 deployment types. Table 9 provides a description of each form of deployment, alongside the number of respondent States and their regional breakdown. The data establish an initial global baseline for current trends in how non-State armed groups, including terrorist groups, have deployed UAS, and the geographical scope of each threat.

62. Non-State armed groups previously had very limited aerial capabilities, such as balloons or hijacked commercial planes. See Chávez and Swed (2020).

63. Global Counterterrorism Forum (2019).

Table 9
Types of attempted or actual deployment of UAS by non-State armed groups

Deployment type	Description of deployment type	Regional breakdown	Total
Attack	The deployment of UAS either (a) to drop or release munitions, or (b) as a loitering munition or single-use attack UAS.	Africa (1), Americas (2), Asia-Pacific (2), Europe (1)	6
Collecting footage to use for propaganda purposes	The high-definition camera payload, which usually comes as default on the latest generation of UAS, can be harnessed to spread propaganda and promote successes. Footage can then be made available online to radicalize supporters.	Africa (1), Americas (1), Asia-Pacific (2), Europe (2)	6
Disruption and interference of critical infrastructure, including air traffic and facilities	UAS disruption and interference can involve simple operations such as flying a commercial off-the-shelf UAS into restricted airspace or it can include the disruption of, and interference with, daily operational practices at sensitive and critical infrastructure such as nuclear power plants, military bases, government offices or energy infrastructure.	Africa (1), Americas (2), Asia-Pacific (2), Europe (2)	7
Distraction or disruption of law enforcement	UAS can be utilized to distract law enforcement. For example, during hostage situations UAS have been used against command posts, creating a distraction that allows perpetrators to flee. They have also been used to disrupt law enforcement, with the presence of UAS above an active crime scene or sensitive site bringing ground operations to a halt.	Africa (1), Americas (1), Asia-Pacific (2), Europe (1)	5
Electronic/signal operations (e.g. cyberattacks and data captures)	UAS can be used to send, receive or relay messages by 3G, 4G or 5G transmitters, or to capture data (such as metadata or communications signals). Due to the modular design of UAS, they can also be fitted with systems that facilitate hacking of television or computer systems, spoofing of Wi-Fi or intranet signals and the hacking of sensitive state systems.[a]	Africa (1), Asia-Pacific (1), Europe (1)	3
Illicit transfers and smuggling of illicit goods	UAS can be, and have been, harnessed to smuggle illicit or restricted materials – such as mobile phones, drugs and weapons – into prisons. UAS have been used to monitor border patrols.	Africa (1), Americas (2), Asia-Pacific (1), Europe (2)	6
Inciting panic at mass gatherings	Due to the potential for a UAS to carry an explosive or CBRN payload, even an unarmed UAS has the potential to disrupt and endanger civilians and cause mass panic at large gatherings, such as major State or sporting events or civil protests.	Africa (2), Asia-Pacific (1)	3
Intelligence, surveillance and reconnaissance	UAS can be deployed to gather intelligence, typically on State practices. In this context, the UAS (usually unarmed) can be used to track the movement of State military forces, conduct reconnaissance or pick out vulnerable targets ready for attack.	Africa (2), Americas (3), Asia-Pacific (3), Europe (2)	10
Swarm	The term "swarm" is commonly used as a broad-brush term to describe the en masse deployment of UAS (in numbers greater than one).[b]	Asia-Pacific (2), Europe (1)	3
Targeted killings	Weaponized UAS can be deployed against a high-value target, such as a Head of State, senior military officials or law enforcement personnel.	Americas (1), Asia-Pacific (2), Europe (1)	4
Targeting support	UAS can aid non-State armed groups in enhancing the precision, destructive capacity and lethality of kinetic strikes. For instance, unarmed UAS can be used to loiter over a target offering both near real-time intelligence, but also post-strike reporting and adjustment.	Africa (2), Asia-Pacific (2), Europe (2)	6
Other	Deployment types not addressed by the above definitions. States were invited to provide details about how non-State armed groups operating in their State deployed – or attempted to deploy – UAS.[c]	Americas (1), Asia-Pacific (1)	2

a. See Rogers (2019).

b. "Swarm" is a contested term in security literature. A breakdown of the differences between en masse deployment and "true" swarms is provided in the section on Outlier approaches, below.

c. States did not provide further information under this deployment type. An example of an alternative deployment mode, not included in this study, is the use of UAS by criminal groups to spread infected biological material to hasten the transfer of disease among livestock, as has been reported in China in 2019; see Zhang and Daly (2019).

The data gathered for this study show a varied set of scenarios in which UAS have been deployed by non-State armed groups, including terrorists, around the world. The most common practices of UAS deployment reflect traditional military practices, such as surveillance and reconnaissance, or kinetic strikes against a varied set of targets. This study also identified other forms of deployment, such as inciting panic and disruption of critical national infrastructure, which are indicative of a much broader, novel range of threats posed by the deployment of UAS by non-State armed groups, including terrorists.

Two States that are heavily affected by non-State use of UAS cited experiencing all except one of the 11 deployment types: one country in Asia-Pacific (which reported observing all except "illicit transfers and smuggling of illicit goods") and one country in Europe (which reported all deployment types apart from "inciting panic at mass gatherings"). Three countries reported not having observed any of the deployment types. Figure 16 shows the proportion of respondent States in each region that observed the deployment of UAS for a particular use. This analysis, despite a small sample of 21 Member States, indicates the most observed deployment types in each region, especially with regard to the non-State use of UAS for intelligence, surveillance and reconnaissance across the regions.

Figure 16
Proportion of respondent States in each region that observed deployment of UAS for particular uses

Deployment type	Africa	Americas	Asia-Pacific	Europe
Attack	17%	20%	29%	33%
Collecting footage to use for propaganda purposes	17%	20%	29%	67%
Disruption and interference of key infrastructure, including air traffic and facilities	17%	40%	29%	67%
Distraction or disruption of law enforcement	17%	20%	29%	33%
Electronic/signal operations (cyberattack, data capture, etc.)	17%	0%	14%	33%
Illicit transfers and smuggling of illicit goods	17%	40%	14%	67%
Inciting panic at mass gatherings	33%	0%	14%	0%
Intelligence, surveillance and reconnaissance	33%	60%	43%	67%
Swarm	0%	0%	29%	33%
Targeted killings	0%	20%	29%	33%
Targeting support	33%	0%	29%	67%
Other	0%	20%	14%	0%
Total respondent States	6	5	7	3

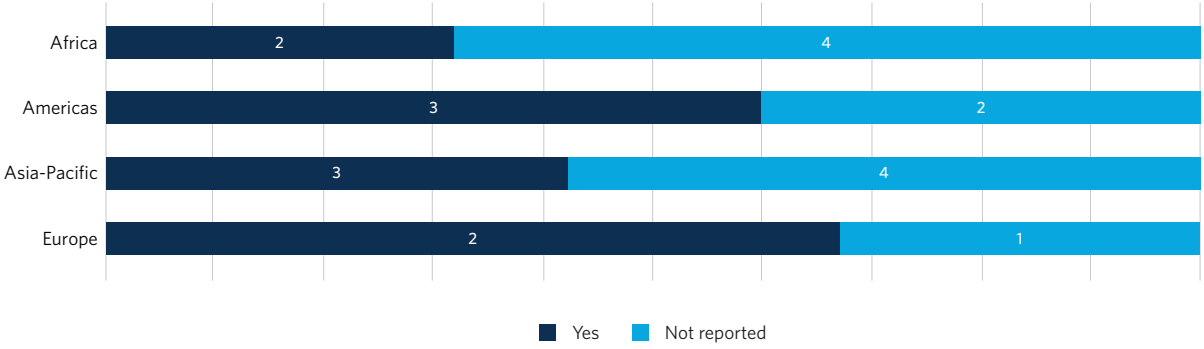
Intelligence, surveillance and reconnaissance

Intelligence, surveillance and reconnaissance was the most reported deployment type overall, with 10 respondent States noting the use of UAS by non-State armed groups for surveillance and reconnaissance-related activities (two of six States from Africa, three of five from the Americas, three of seven from Asia-Pacific and two of three from Europe; see fig. 17). The deployment of UAS by non-State armed groups for intelligence, surveillance and reconnaissance purposes was the most reported deployment type and is thus a key priority and concern for respondent States. The scope of this category is broad, but empirical examples help to highlight the various threat scenarios faced by States. In the United States of America, for instance, human traffickers have used commercial off-the-shelf UAS to gather intelligence on the movements of border patrols, enabling them to evade law enforcement.

This is a tactic adopted by non-State armed groups around the world looking to cross borders undetected, or to gather intelligence on military, security or law enforcement targets before attack. A representative of the United States Customs and Border Protection stated: "Human smugglers using drones to surveil the Border Patrol is a growing trend that we've observed along the border … This technology provides transnational criminal organizations with new capability that they are eager to exploit".[64]

Similar intelligence, surveillance and reconnaissance activity has been reported by United Nations peacekeeping missions, with UAS used to set up ambushes and to coordinate attacks. Officials have recorded UAS being used to conduct surveillance of peacekeeper facilities and patrols in several countries. In an interview with United Nations officials in October 2022, it was revealed that in one African country (in which United Nations peacekeepers are currently deployed), the mission has reported a weekly average of 17 UAS overflights of United Nations facilities.

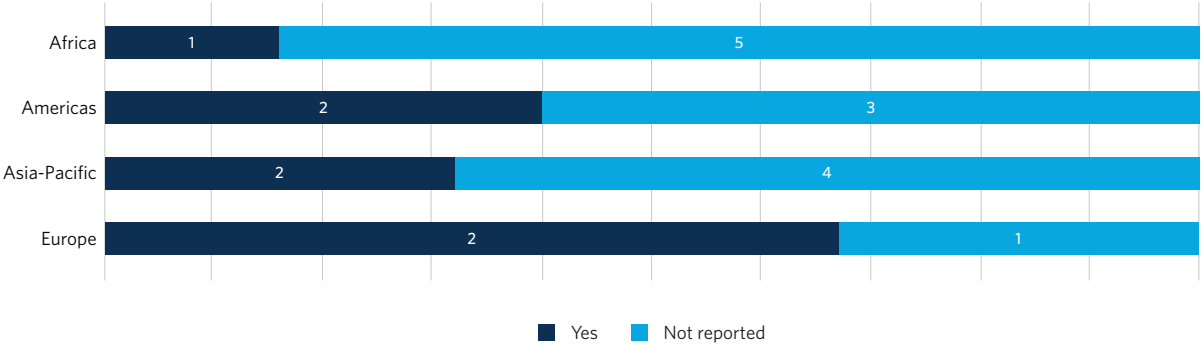
Figure 17
States reporting use of UAS by non-State armed groups for intelligence, surveillance and reconnaissance



Disruption of critical infrastructure

The second most common form of UAS deployment reported by Member States is disruption and interference of critical infrastructure. Seven States reported this (one from Africa, two from the Americas, two from Asia-Pacific and two from Europe; see fig. 18).

Figure 18
States reporting use of UAS by non-State armed groups to disrupt or interfere with critical infrastructure



64. US Customs and Border Protection (2023).

The term "critical infrastructure" was not defined in the questionnaire, and States were invited to apply their own national understanding. It may be understood to broadly encompass several specific target types, including energy utilities such as power stations or dams, or transport locations such as airports and train stations.[65]

Airports were identified by Member States as the most common target of UAS deployment by non-State armed groups (see table 10).[66] Eight States – 38 per cent of respondents – stated that airports had been subject to weaponized UAS strikes or unarmed UAS disruption. This dynamic was particularly prominent in Asia-Pacific: four of the six respondents reported incidents targeting airports. Airports are especially sensitive locations, where even careless or negligent use – as opposed to deliberate terrorist attacks – can pose dire threats to civilian security. At the regional consultations, one State from East Asia remarked that one civilian airport had been subject to 190 illegal UAS flights in 2021 alone, of which 30 per cent had resulted in delayed take-off or landing at the airport, causing fear and anxiety among passengers. In September 2021, INTERPOL and the Norwegian Police held a drone incursion exercise at Oslo Gardermoen Airport, Norway, to test and assess the abilities of 17 counter-UAV systems and determine their effectiveness in ensuring the safety of the airport environment. Among other findings, the exercise showed that there is currently limited knowledge and operational testing data in relation to counter-UAS, and that each counter-UAS installed at a location may need constant or regular adjustments to ensure that it meets the operational needs of law enforcement.[67]

Table 10
Target types

Target type	No. of reporting States	Regional breakdown
Airports	8	Africa (1), Americas (1), Asia-Pacific (4), Europe (2)
Civilian individuals or groups	6	Africa (1), Americas (1), Asia-Pacific (3), Europe (1)
Energy infrastructure and utilities (e.g. power stations, network grids, dams)	4	Americas (1), Asia-Pacific (2), Europe (1)
First responders	3	Africa (1), Asia-Pacific (2)
Government buildings	5	Africa (1), Americas (1), Asia-Pacific (3)
Law enforcements	5	Africa (2), Americas (1), Asia-Pacific (1), Europe (1)
Military buildings or infrastructure	7	Africa (2), Americas (2), Asia-Pacific (2), Europe (1)
Military personnel	6	Africa (2), Americas (1), Asia-Pacific (2), Europe (1)
Other non-State armed groups	4	Africa (2), Asia-Pacific (2)
Other transport infrastructure (e.g. roads, railways, stations)	6	Africa (1), Americas (1), Asia-Pacific (3), Europe (1)
Populated areas and public spaces ("soft targets" e.g. markets, stadiums, religious or cultural sites)*	5	Africa (1), Asia-Pacific (3), Europe (1)
Prisons	5	Americas (2), Asia-Pacific (1), Europe (2)

* See www.un.org/counterterrorism/vulnerable-targets and www.un.org/counterterrorism/fr/node/20481.

65. At the eighth review of the Global Counter-Terrorism Strategy, the General Assembly called upon Member States to "strengthen efforts to improve the security and protection of particularly vulnerable targets, including religious sites, educational institutions, tourist sites, urban centres, cultural and sport events, transport hubs, rallies, processions and convoys" (see General Assembly resolution 77/298).

66. For more information on critical infrastructure and public places/soft targets protection, see www.un.org/counterterrorism/vulnerable-targets.

67. INTERPOL and Norwegian Police (2022).

ICAO is a specialized agency of the United Nations that coordinates and advises Governments in their implementation of the 1944 Convention on International Civil Aviation. Among other UAS-related activities, ICAO provides guidance to States to support their efforts to protect civil aviation infrastructure from the use of UAS.[68] In an interview with ICAO experts in November 2022, it was stressed that effective prevention of UAS incidents "heavily relies on a multidisciplinary approach, both preparedness and response. There is no silver bullet; the key for us is to provide a forum where everyone can work together and share experiences". The guidance from ICAO to States includes an incursion threat assessment form, as well as examples of State's decision-making processes to determine the level of threat from a UAS. ICAO recommends that States and airport operators develop their own threat assessment tools to inform an appropriate and proportionate decision-making process to respond to prospective UAS threats, taking into account factors such as the behaviour and intent of the craft, and the credibility of the sighting.[69]

Other infrastructure targets also feature prominently in table 10, including transport infrastructure (six States) and energy infrastructure and utilities (four States). These sensitive sites can pose challenges for States in terms of counter-UAS protection. At the regional consultations in January 2023, one European State observed that in September 2022, for the first time, sightings of UAS were reported offshore near national oil and gas fields. The purpose and operator behind those systems were unclear, but the State noted that deploying effective countermeasures was complicated by the fact that the UAS were operating both in international airspace and international waters.

The UNOCT Global Programme on Countering Terrorist Threats against Vulnerable Targets – in partnership with CTED, UNICRI and UNAOC – has published guidance on protecting vulnerable targets – including critical infrastructure and public places ("soft targets") from terrorist attacks involving UAS. This guide examines, through a selection of case studies, tools and resources, how different stakeholders can contribute to preventing and addressing the UAS threat to vulnerable targets, including by developing public-private partnerships.[70]

"Unarmed and dangerous"

Targeting support, collecting footage to use for propaganda purposes, and illicit transfers and smuggling of illicit goods via UAS were each reported by six States, making them joint third in terms of overall trend reporting. These three diverse deployment types are united by the fact that they can be conducted by unarmed, non-weaponized UAS. They each are functions that non-State armed groups can implement through other means but are rendered far more potent and effective by being conducted aerially, with hard-to-detect and highly capable UAS.

68. ICAO includes remotely piloted aircraft, small UAS ("drones"), model aircraft and unmanned free balloons and makes a distinction between unmanned aircraft that can be accommodated in airspace by keeping them away from other aircraft, and those that act like, and are treated like, manned aircraft. ICAO has prepared a UAS toolkit that compiles best practices and regulations in support of Member States' efforts to develop effective operational guidance on the use of UAS (available at www.icao.int/safety/UA/UASToolkit/Pages/default.aspx).
69. ICAO (2020).
70. This guide is available in Arabic, English, French and Russian at www.un.org/counterterrorism/fr/node/20481.

The Center for the Study of the Drone at Bard College, United States, has coined the term "Unarmed and dangerous" to refer to the lethal applications of non-weaponized UAS, including target acquisition and targeting support. This is where UAS are used to enhance the accuracy and destructive capacity of a kinetic strike via a conventional mortar, rocket or artillery. The same UAS can then be used to observe and report on a strike's effectiveness, and the video recorded can be used for propaganda purposes.[71]

UAS can also bypass traditional border checks or security apparatus to supply lethal weapons or illicit goods, which should be considered another dangerous element of unarmed UAS deployment by non-State armed groups. In an interview with a WCO representative in April 2023, the use of UAS by non-State armed groups to monitor borders to change and adapt their smuggling routes, or else to harass and distract UAS deployed as security measures on national borders, was also identified.

BOX 9: MONITORING, RECORDING AND UNDERSTANDING THE PROBLEM OF NON-STATE USE OF UAS

Of the 21 respondent Member States, 14 reported that they maintained a national database of UAS incidents and attempted incidents. The national intelligence services are most often reported as the agency type responsible for managing these databases. Two States cited specialist counter-UAS centres or teams in which this function is housed. Three cited civil aviation authorities as the national custodian of data recording. Eight of the 14 countries cited multiple agencies, suggesting that different authorities kept different relevant data.

All 14 States indicated that they recorded information related to:

- Actors responsible
- UAS type involved
- Incident target type
- Physical damage or casualties resulting from the incident.

Only eight States reported that they recorded information on the gender-disaggregated impacts of UAS incidents. In addition, one State reported that they recorded information related to motivations and capabilities (financing, access to equipment).

INTERPOL, as part of providing support to its member countries, has developed a voluntary drone incident reporting template. This template can be adapted according to the national context. It contains 27 fields, including those related to the incident, the UAS, its behaviour, recoveries and which counter-UAS was used.

71. Holland Michel (2020).

Outlier approaches

The three least observed forms of UAS deployment were "inciting panic at mass gatherings", "electronic/signal operations",[72] and "swarm" attacks. The latter two, in particular, may reflect advanced capabilities outside the reach of most non-State armed groups and requiring a significant level of expertise to deploy. Three respondent States – one in Africa, one in Asia-Pacific and one in Europe – reported non-State armed groups using, or attempting to use, UAS in electronic or signals operations. Likewise, three States cited the use of UAS by non-State armed groups to incite panic at mass gatherings: two in Africa and one in Asia-Pacific. No further information was provided by those States. However, at an interview in October 2022, United Nations officials noted a similar dynamic in operations where United Nations peacekeepers are deployed. In one instance, a UAS was reported to chase people into a camp hosting internally displaced persons. The harassment of vulnerable civilians in this context was noted to be intended to incite panic within the camp.

The three States that reported experience of actual or attempted swarm attacks were all engaged in conflict with non-State armed groups that were well documented to have powerful State support and advanced UAS capabilities. The term "swarm" is highly contested among security theorists. It is commonly used as a broad-brush to describe the deployment of UAS en masse, or just in numbers greater than one. Swarm attacks involve the launching of numerous unconnected and unlinked UAS towards a target to overwhelm and saturate air defence systems and destroy the intended target. This has been seen used against energy infrastructure and military bases.[73] For the purposes of this report, this broad description will be adopted, but it should be noted that an en masse deployment of UAS is not a true technical UAS swarm. A true swarm presents a set of unique threats that are not apparent in less high-tech mass deployments. It is the ability of UAS to communicate with each other that marks a true swarm from an en masse deployment. The communication element allows for collaboration as a concerted unit. For example, while an en masse deployment of UAS may be able to overwhelm air defence, a communicating UAS swarm will be able to monitor external stimuli and react to the sensors of other UAS to evade incoming air defence systems. Therefore, a true UAS swarm will present novel dangers that can overcome, overwhelm or exhaust the current generation of counter-UAS.[74]

72. Such activities may include GPS spoofing, hacking electronic systems and infrastructure, spreading disinformation and capturing information from sensitive sites; see Rogers (2019).

73. See, for example, Reid (2018).

74. For more information on swarm technology, see Ekelhof and Persi Paoli (2020); Kallenborn (2022); Kallenborn, Ackerman and Bleek (2022); and Verbruggen (2019).

BOX 10: DRONE MANAGEMENT PLAN

At the regional consultations, the challenge of timely and accurate detection of a hostile UAS was a recurrent theme among State interventions. One State in East Asia described how it had instituted a Drone Management Plan to provide a framework for decision-making in scenarios where such a detection must be made.

This plan was introduced after it observed that the traditional military approach of "detect, track and defeat" was not suited to the UAS threat. In part, this was because of a case where suspicious UAS were deployed in populated areas, and UAS countermeasures were not considered appropriate. Instead, a new approach was introduced: "detect, observe and manage". Within this framework, considerations are guided by a basic checklist of questions:

1. Is it a drone?
2. What type of drone?
3. What does it carry?
4. What is the purpose?
5. Is it a manual or autonomous flight?
6. Can the location of the drone pilot be specified?

From the moment a suspected drone is detected, observation is initiated, the length of which is dependent on the perceived urgency and state of emergency. The checklist is used to help reach a determination about the threat level and make an initial assessment. If a threat is deemed to be low, the UAS is observed for 20 minutes. If it is deemed medium, observation continues, and the threat is reported to the relevant agencies. If it is deemed to be high, alert notifications are issued, and the threat is immediately reported to the relevant police or military bodies to initiate a response.

Member State priority concerns

Two key concerns emerged at the consultations. The first is the use of UAS to carry out direct kinetic attacks, particularly through the use of IEDs or dropping of conventional munitions. Within this, a specific threat dynamic that was highlighted as a particular concern was the use of UAS in targeted killings of high-value, high-profile and high-status individuals. In recent years, there have been several incidents of attempted assassinations of political figures, such as against President Maduro in the Bolivarian Republic of Venezuela in 2018, the dropping of aerial explosives on the home of Prime Minister al-Kadhimi in Iraq in 2021 and the Taliban's reported assassination of an ethnic Uzbek warlord in Afghanistan in 2021.[75] Several States referenced this deployment type. As a national security expert from a Member State in Asia-Pacific said:

> In my view one of the main concerns with the terrorist use of drones would be VIP assassination attempts. If you're moving the Head of State or another important person from Point A to Point B, you might have quite good ability to not have other vehicles get close; you might have plotted the route you'll be taking; you can check that there aren't enemy snipers. But if something just flies in – it might have been left on [the roof of a nearby] building, unnoticed under a sheet of cardboard – and then out it comes, flies straight to the vehicle, and detonates. That's something that unfortunately could be quite an effective attack vector.

For the second, two States from the Asia-Pacific region separately highlighted concern about the increasing use of UAS by non-State armed groups to target maritime vessels and infrastructure, including ports. An example of this dynamic is described in the deployment case study. This may not be a common threat currently, but it was cited by both the national authorities from the two Asia-Pacific States as having a particularly damaging strategic and economic impact in the Gulf region, considering the significance of those shipping channels for international commerce, as well as the potential for rapid escalation in a highly sensitive maritime location. As one expert noted:

> When we think about terrorist use of UAS, we tend to think about land. But we have seen attacks against vessels in the Persian Gulf, and this is a big threat. It means that you are bringing this danger to one of the most crucial places in the world, not just in terms of commerce but also specifically transportation of energy.

75. Schori Liang (2023).

BOX 11: EXAMPLES OF NATIONAL PRACTICE TO COUNTER UAS DEPLOYMENT BY NON-STATE ARMED GROUPS

Of the 21 respondent Member States, 13 reported that they had a national policy to counter UAS. This included all six States from Africa, three of five States from the Americas, two of six States from Asia-Pacific (one of which noted exceptions but did not clarify further) and two of three States from Europe.

Eight States said that they had a designated counter-UAS coordinating lead entity. These sat under various agency types, including:

- A dedicated inter-agency committee or national centre for UAS, bringing together different law enforcement agencies and government bodies
- Civil aviation authorities
- National security or intelligence agencies
- Specific government ministries (e.g. interior or transport ministries).

Of the 21 respondent States, 17 stated that their national authorities imposed no-flight zones for UAS, preventing deployment in specific locations. Only one responded "no" to this question, while two did not submit a response. Airports, military sites, government buildings and critical public infrastructure featured prominently among the locations reported as being subject to such restrictions.

A set of good practices for protecting vulnerable targets from terrorist attacks involving UAS has been compiled by the UNOCT Global Programme on Countering Terrorist Threats against Vulnerable Targets (available at www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf).

Figure 19

Parts of a UAV recovered in 2018 from a non-State armed group. The UAV consisted of commercially available components and a locally manufactured airframe (documented by CAR field investigators in July 2018)

VII. Case study: deployment[76]

Use of UAS in Yemen

According to field investigations conducted by CAR, since 2016, Ansar Allah ("Houthi") forces have deployed UAS in an increasingly lethal fashion in Yemen and neighbouring countries.[77] As the technological capabilities of the systems in the group's possession have become increasingly complex, the group has become more ambitious in their deployment approaches and attack profile. The group's deployment of UAS has undergone at least four distinct stages (see table 11), each distinguished from the others in terms of scale, ambition and target type.

First, Houthi forces initially used small, commercially available UAS to conduct intelligence, surveillance or reconnaissance activities. The first reported incident in the country involved a small quadcopter that had been allegedly stolen from a local television studio.[78]

Second, in October and November 2016, Houthi forces crashed several unsophisticated UAVs into missile defence systems in Yemen in order to disable the radar antennas. They then launched a missile attack that the damaged systems were unable to intercept.[79] Houthi forces increasingly used these UAS in attacks against coalition ground forces operating in Yemen. The Security Council Panel of Experts reported 11 UAS attacks in Yemen against ground forces between 1 December 2016 and 17 January 2017.[80] These systems were relatively rudimentary, involving a single battery power source, crudely installed circuitry and with a maximum range of 150 km. The Panel of Experts determined that it was not a precision weapon, capable only of gliding to its pre-programmed target location.[81]

Table 11
Stages of UAS deployment in Yemen 2015–2022

Stage	Year	Deployment type	UAV type
1	2015	Surveillance and reconnaissance	Small commercial quadcopter
2	2016	Direct attacks on missile defence systems and ground forces	First-generation UAV with >150 km maximum range
3	2018	Long-range attacks, including on civilian airports in neighbouring countries	UAV with >1,500 km maximum range
4	2021–2022	Strategic attacks on economic and energy infrastructure	Larger UAVs capable of carrying two munitions

76. The case studies are drawn from field investigations conducted by CAR. Although they illustrate specific examples of deployment efforts, they are distinctive to specific contexts in which CAR operates, and are not representative of all issues relating to, and arising from, the deployment of UAS by non-State armed groups. The field investigations have not been verified by the United Nations.
77. The Security Council referred to the Houthis as a terrorist group for the first time in its resolution 2624 (2022), operative para. 1.
78. Muhsin (2019).
79. These UAS allegedly entered Yemen overland through a weapons smuggling route transiting the territory of a neighbouring state. See CAR (2017a); and S/2018/68, para. 98.
80. S/2018/68, annex 37.
81. S/2018/68, annex 38.

The third stage became manifest in September 2018, when investigators first documented a new model, with a more powerful engine capable of launching attacks over much larger ranges, up to 1,500 km.[82] They were also capable of carrying a larger payload (in this instance, warheads weighing 18 kg of explosives mixed with ball bearings). Equipped with more powerful systems, Houthi forces expanded to attack more ambitious targets with a high symbolic impact, including civilian airports in Saudi Arabia and the United Arab Emirates.[83] Between April 2018 and August 2021, Abha International Airport – in the southern Asir Province of Saudi Arabia – suffered 18 successful aerial attacks involving UAVs and cruise missiles. Two people were killed in the attacks, and a further 77 were injured.[84]

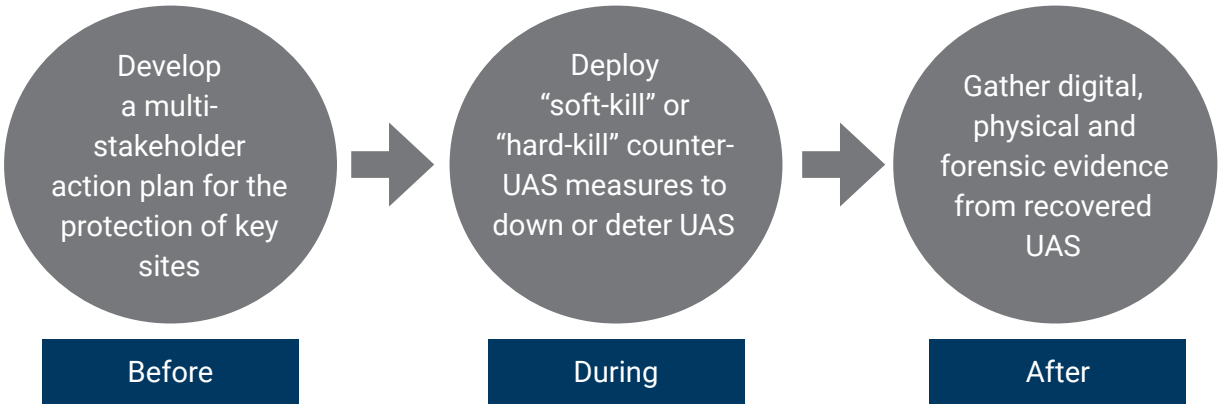
Attacks in 2021 and 2022 signal a fourth type of UAS deployment pursued by Houthi forces: attacks against economic and energy infrastructure, primarily maritime targets. The most recent of these took place in October 2022, when Houthi forces used two UAVs in an attack reportedly intended to prevent a tanker from loading oil at the Ash Shihr port near the city of Mukalla.[85] The Government of Yemen reported that this was the third UAV attack against shipping that week. Similar UAV attack attempts were carried out in November 2022 against ports in the governorates of Shabwah and Hadramawt.[86] Those attacks may have involved larger numbers of UAVs, deployed alongside missiles, to target strategically and economically significant sites.[87]

Countering UAS deployment

This case study is distinct to Yemen. Each non-State armed group has its own pathway and develops its capacity according to distinct operational imperatives. Therefore, the intervention points relevant to each deployment of UAS will be unique to the situation. In terms of general preventative measures, several measures may be broadly relevant to all non-State deployment of UAS. First, developing a multi-stakeholder action plan to protect sensitive national infrastructure, such as civilian airports or energy infrastructure sites. Member States highlighted the importance of close cooperation between civil aviation, law enforcement and the military to regulate airspace and prevent attacks. Technically, the implementation of counter-UAS that can affect soft or hard "kills" of UAS may be part of such an action plan. An area where States have expressed interest in receiving training and capacity-building support relates to procedures for recovering, analysing and preserving evidence following a UAS incident. This includes physical, biometric and digital forensic capabilities that would help to inform law enforcement investigations and, ultimately, judicial proceedings.

82. CAR (2020a).
83. S/2019/83, paras. 84–86.
84. S/2022/50, annex 17.
85. Al-Haj (2022). This information was corroborated in an interview with a representative of the Government of Yemen on 16 March 2023, according to CAR.
86. Jalal (2023)
87. See, for example, the Panel of Experts' investigations into the Mukha Port attack on 11 September 2021, which reportedly involved two missiles and six UAVs (S/2022/50, annex 8).

Figure 20
Intervention points to counter terrorist deployment of UAS



VIII. Conclusion: tackling terrorist use of UAS

The increasing use of UAS by non-State armed groups poses a grave security threat to Member States around the world. The threat is not isolated to countries facing armed conflict. This research has identified four principal global trends relating to how non-State armed groups, including terrorists, access and use UAS.

First, non-State armed groups, including terrorists and criminal groups, are primarily exploiting commercial sources to access UAS. These commercial access points may be acquired legally in some cases, or illicitly trafficked in others. Legal holdings – whether government or private – are currently not regarded as key sources of diversion of UAS.

Second, while more advanced UAS capabilities currently lie outside the reach of many non-State armed groups, there is evidence that some have been able to establish local industrial capabilities.

Third, non-State armed groups could be – and in some cases already are – sharing this knowledge with other organizations. The transfer of knowledge, whether in person or online, is a critical transmission vector that could greatly speed up the proliferation of UAS weaponization in other contexts.

Fourth, due to the relative ease of access to UAS materials and knowledge, a growing number of non-State armed groups may be able to conduct attacks with weaponized UAS. To date, the dominant uses of UAS have been with unarmed systems, such as surveillance, trafficking or target acquisition. There is, however, a serious threat that future attacks will not only increase in frequency and geographic scope but also increase in range, precision and power as non-State armed groups pursue more advanced capabilities.

Looking forward, there are several features of this threat that may rapidly evolve in prominence and complexity in the future. These include growth in autonomous flight capabilities, including through AI; enhanced data transfer and communication capabilities; modifications to include dispersal or spraying mechanisms; more advanced power sources to increase flight range and speed; and the ability of non-State groups to override manufacturer "fail-safes". In addition, one emergent threat not reported by States but that could greatly complicate efforts to counter the non-State use of UAS is the rapid development of underwater and on-land unmanned systems.[88] Reports on future trends should revisit these emergent threats to see whether those forecast concerns materialize.

Both in the rapid growth in availability, and the "cat and mouse" nature of weaponization, broad parallels can be drawn to other novel technologies that terrorists have utilized in the past. Hence, it may be relevant and helpful to look towards approaches developed to address other new "game changer" technologies in the hands of terrorist actors. Perhaps most notably, the counter-IED domain may have valuable lessons for stakeholders concerned by the prospects of increasing use of UAS by non-State armed groups. For example, the Joint Improvised

88. Grand-Clément and Bajon (2022b).

Explosive Device Defeat Organization, founded in 2006 in response to the growing threat of IED use by non-State armed groups, developed three lines of operation to form a framework for a counter-IED approach: (1) attack the network; (2) defeat the device; and (3) train the force.[89] Transferable lessons may be applicable to efforts to prevent terrorist access to UAS.[90] In fact, at least one United Nations agency is already adopting this approach in their operational efforts to counter non-State threats relating to UAS.

The consultations with Member States and other expert stakeholders highlighted a range of intervention points relevant to countering the non-State use of UAS, including by terrorists. States are either already implementing these measures to prevent or mitigate UAS use by non-State armed groups or else these ideas emerged during the consultations as examples of good practice that could be considered for implementation by States and other stakeholders. UNOCT and CAR have consulted other key guidelines and frameworks, and integrated the findings of the present study to create a list of identified good practices (the "threat reduction framework"; see table 12). This framework could serve as a reference tool to help Member States and other relevant stakeholders to consider ways to counter the non-State use of UAS across the pillars of acquisition, weaponization and deployment.

The good practices can be grouped into six key policy areas: (1) national laws, policies and procedures; (2) supply chain security measures; (3) information management and sharing; (4) counter-UAS measures; (5) monitoring and diagnostics; and (6) multilateral initiatives, cooperation and assistance. The policy areas identified are not intended to be exhaustive of the measures that can be taken to address the terrorist use of UAS, or specific recommendations for specific Member States or other stakeholders. Rather, they represent a framework of possible actions that can be taken by States and could form a basis for further research into (a) global uptake, (b) continuing relevance and (c) gaps and new or alternative action areas.

1) National laws, policies and procedures

The coordination of legislative, regulatory and national efforts is essential for an effective, whole-of-community response to the threat of non-State use of UAS, including for terrorism-related purposes. The development of a national action plan to counter non-State use of UAS, for example, would bring together stakeholders from law enforcement, regulatory and civil aviation authorities, customs, industry and civil society, among others. Moreover, national coordination and stakeholder engagement have been identified as good practices in addressing the terrorist use of UAS. Such coordination would clearly define roles and responsibilities, integrate all relevant stakeholders, and build a collective whole-of-community approach to tackling this problem.

89. "Attack the network" focuses on disrupting the complex network of financiers, trainers and their supporting infrastructure that facilitates IED use. "Defeat the device" involves providing technologies to detect IED components, neutralize triggering devices and mitigate the effects of an IED blast. "Train the force" centres on improving the knowledge and proficiency of deploying forces. For more information, see Martin and others (2013).

90. For example, as noted by UNIDIR in 2020: "Probably the most effective upstream counter-IED measure is to use proactive intelligence to interdict individuals or groups before they can manufacture and deploy IEDs" (Seddon and Malaret Baldo (2020)).

2) Supply chain security measures

Preventive measures to strengthen supply chain security for commercial off-the-shelf UAS, or for UAS components, could help to tackle the threat of terrorist and non-State use of UAS at its source. While some Member States expressed doubt that it would be possible or productive to seek to prevent the acquisition of UAS technology fully – especially in view of the ability of some groups to manufacture vehicles from low-tech items – others promoted reducing the ease of access to UAS materials as a key action area in which to focus collective efforts. Steps to ensure supply chain security might include requiring enhanced risk assessments for transfers of UAS and UAS components; ensuring that this material is uniquely marked and that serial number-level records are kept by transfer parties across the supply chain; and that counter-diversion efforts for conventional ammunition and IED precursors are strengthened to stop terrorists and other non-State armed groups from accessing material required to weaponize UAS.

3) Information management and sharing

At the consultations, information-sharing emerged as one of the most requested and endorsed strategies at the multilateral level to address the terrorist and non-State use of UAS. Member States repeatedly highlighted the importance of dedicated forums to share operational insights and learn from national experiences. Where States identify emergent trends, these platforms may provide an "early warning" function. Close cooperation between States and industry was also emphasized as an example of good practice in this policy area, such as through the provision of advance notifications of emerging product innovations that would empower regulators and law enforcement to prepare appropriate responses.

4) Counter-UAS technical measures

The term "counter-UAS" refers specifically to countering UAS use by non-State armed groups, including terrorists, and is not oppositional to UAS use by States and other legitimate custodians.

One key theme that emerged from consultations for this study was that there is no single one-size-fits-all solution for countering the non-State use of UAS. Consequently, this policy area includes five identified sub-areas: (1) conducting regular threat and vulnerability analysis to assess the impact of new developments, in particular emerging technologies, on existing countermeasure approaches; (2) developing counter-UAS capability, which includes establishing, testing and maintaining technical counter-UAS, and training the appropriate personnel in its through-life management and use; (3) conducting UAS incident safety and security measures; (4) developing recovery and technical exploitation capabilities; and (5) establishing appropriate criminal justice processes consistent with national law as a deterrent and enforcement measure against actors evidenced to be advancing the non-State use of UAS.

5) Monitoring and diagnostics

The fifth policy area relates to the ongoing challenge of accurately assessing the scale of UAS use by non-State armed groups. Monitoring and diagnostic activities may include developing a coordinated, multi-stakeholder database of national UAS incidents; conducting and supporting end-use or end-user monitoring activities for diverted UAS; tracing UAS and UAS components; establishing a dedicated national research centre related to countering threats from UAS;

and investing in new or existing civil society and academic initiatives to research and gather evidence on the scale and nature of the threat posed by the non-State use of UAS.

6) Multilateral initiatives, cooperation and assistance

The final policy area is cross-cutting across the framework and covers two key areas. The first relates to multilateral initiatives to reinforce and strengthen global norms against the non-State use of UAS. States expressed support for concerted collective action against the proliferation of UAS capacities to non-State armed groups. This included calls for the development of dedicated international frameworks to restrict access to UAS components, and for the reinforcement of collective pressure, including through sanctions packages to deter and stigmatize proliferators. Second, several States cited the need for greater international support and technical assistance to countries facing UAS threats from non-State armed groups, including through training in UAS recovery, documentation, exploitation and tracing.[91] This study has therefore identified measures relating to the provision of technical, financial and legal assistance, including through multilateral efforts such as the AROS Programme, as a cross-cutting good practice to support all relevant stakeholders in collectively and effectively countering the threat of UAS used by non-State armed groups, including terrorists.

91. In the wider context of protection of vulnerable targets, and interaction with UAS, the Global Network of Experts was launched in 2022. Currently, it has 200 experts from more than 70 Member States, international and regional organizations, civil society, academia and the private sector. For more information, see www.un.org/counterterrorism/events/launch-united-nations-network-experts-protection-vulnerable-targets-against-terrorist-attacks.

Table 12
Good practices to reduce the threat of non-State use of UAS (the counter-UAS threat reduction framework)

Policy areas	General	Acquisition	Weaponization	Deployment
1. National laws, policies and procedures				
1.1. Policy and strategy	Develop a national action plan that establishes a comprehensive, whole-of-government approach to prevent, protect against, respond to, recover from and mitigate against the use of UAS by non-State armed groups, including for terrorism-related purposes.	Develop specific strategies to counter acquisition networks that supply UAS and related technologies to non-State armed groups, including for terrorism-related purposes.		Develop specific crisis management strategies that mitigate the impact of UAS incidents. Develop a multidisciplinary action plan for the protection of vulnerable targets, including critical infrastructure and public spaces, and "soft targets", from the use of UAS, including for terrorism-related purposes.
1.2. Legislation and regulation	Establish regulations covering the acquisition and use of UAS by non-State armed groups, designed to prevent and mitigate the threats posed by malicious, criminal and terrorist use of UAS and components. Periodically review existing legislation and regulations, taking into account new technological developments pertaining to UAS and related technologies, among other factors.	Register and license manufacturers of UAS and critical UAS components, to mitigate the risk of unlicensed or illicit production. Consider stipulating manufacturer-level controls and precautions against the malicious, criminal or terrorist use of UAS. Define restrictions or limitations on the acquisition of certain types of UAS and related technologies by non-State armed groups. Such restrictions should specify the types of UAS, associated components or subsystems that are to be controlled.	Integrate into existing legislation or regulations a prohibition against the possession of materials, knowledge or equipment relating to the weaponization of UAS by non-State armed groups.	Enact regulations that establish appropriate limitations on the operation of UAS, as well as the designation of restricted airspace zones and limits. These regulations may pay particular attention to restrictions regarding specific people (e.g. emergency services, national security and law enforcement) or infrastructure (e.g. airports, public gatherings, stadiums and energy utilities). Establish licensing requirements for operators. Register operators, aircraft or both.
1.3. National coordination and stakeholder engagement	Establish or designate a national coordinating lead entity and points of contact across and within all concerned national authorities at different levels (national, subnational and local) to promote coherent cross-government approaches to countering threats posed by the terrorist use of UAS, as well as ensuring effective coordination in response to an incident. Promote a whole-of-community approach to prevention and preparedness against the non-State use of UAS by instituting policies and practices that encourage engagement across government, industry and the private sector, academia, civil society, and research institutions.	Promote public-private partnerships in deterring and addressing the illicit acquisition networks that supply terrorists with UAS and related technologies.		Establish or designate competent and responsible national authorities that are authorized to detect and, if necessary, intercept and/or disable UAS and components.

Table 12 (*continued*)

Policy areas	General	Acquisition	Weaponization	Deployment
2. Supply chain security measures				
2.1. Marking and record-keeping		Establish adequate through-life inventory management systems for UAS. Ensure comprehensive record-keeping for transfers of UAS and related technologies across the supply chain, where consistent with national laws. Put in place record-keeping policies and practices for lost and stolen UAS and related technologies. Uniquely label UAS and critical UAS components, including – where possible and feasible – addition of end-user identifiers on systems and essential components. Consider, where appropriate, integrating in-built tracking within high-value UAS and UAS components (e.g. motors, gyroscopes and agricultural UAS) at production or post-production stages.		
2.2. Physical security of systems, components and associated materials		Ensure secure storage, handling and transport of UAS, in particular armed UAS, and related components to prevent their diversion to unauthorized recipients. Establish physical security policies and procedures for certain types of UAS and their critical components of highly sensitive nature, as appropriate.	Secure lawful State and non-State holdings of materials that can be used to weaponize UAS, paying particular attention to the secure storage of conventional ammunition, explosives and precursors to prevent their diversion to unauthorized recipients. Prioritize the physical security of conventional ammunition containing high quantities of explosives, whose acquisition may be attractive to non-State armed groups, including terrorists.	

2.2. (*cont'd*)			Safeguard or clear usable cached, abandoned and uncleared conventional ammunition for the specific purpose of denying its acquisition by non-State armed groups, including terrorists. Prioritize clearance of unexploded ordnance and the safeguarding, safe storage, recovery, or disposal, and preferable destruction of unguarded legacy or obsolete stockpiles of conventional ammunition that are still operational to deny access to conventional ammunition by non-State armed groups, including terrorists.
2.3. Transfer control of systems and components		Regulate the international transfer of armed UAVs in line with national export control frameworks. As part of transfer authorizations of armed UAVs, require the routine use of end-use or end-user assurances such as a commitment not to re-export transferred UAS without prior approval by the original supplier. Review and consider the integration of critical and highly sensitive UAS components into national export control frameworks, including comprehensive risk assessments. Promote development of codes of conduct and other due diligence and compliance activities by industry and private sector actors, to prevent diversion of UAS and related technologies to non-State armed groups, including terrorists.	Regulate the international transfer of conventional ammunition in line with national transfer control systems. Prior to transfer, assess the risk of diversion of materials that can be used to weaponize UAS. Encourage States and the private sector to increase prevention efforts, by taking measures to stem the transfer of knowledge of the construction of weaponized UAS and their use by non-State armed groups.
2.4. Customs and border control	Build specialized expertise and capacity for border and customs officials to identify and seize diverted UAS and related technologies at customs and border points.	Encourage national law enforcement, customs and border control authorities to collect data on seized and recovered UAS and related critical components.	

Table 12 (*continued*)

Policy areas	General	Acquisition	Weaponization	Deployment
3. Information management and sharing				
3.1. Intelligence gathering and sharing	Encourage close cooperation and information exchange, as appropriate, among parties investigating UAS diversion and misuse, including national law enforcement; defence forces; customs and border control; export and import licensing authorities; intelligence services; international and regional law enforcement organizations; regional law enforcement organizations; relevant regional entities; and relevant United Nations entities.	Promote close cooperation and coordination between the State's intelligence entities, law enforcement and specialist military support agencies for the prosecution of time-sensitive intelligence-led operations against individuals involved in the procurement, development and operation of UAS and components by terrorist groups. Gather information on methods of shipment, means of concealment and routes customarily identified as used by organized criminal groups and terrorist organizations engaged in UAS diversion, and on the specific types of UAS and critical components recovered by security forces. Consider sharing information on seized and recovered UAS or critical components with a view to enhancing cross-border law enforcement cooperation and promoting more effective counter-diversion and counter-trafficking measures. Report data on seizures of UAS and UAS components to the WCO Customs Enforcement Network. Maintain registers and databases of actors and entities (e.g. manufacturers, brokers, vessels and aircraft, as well as end users, shippers and freight forwarders) that have a history of diversion or poor security measures relating to UAS.	Establish a national mechanism or process to enable early-warning monitoring of new UAS-related capabilities that could be used for terrorism purposes. Establish operational information-sharing relating to the movement of individuals with expertise in weaponizing UAS technologies. Promote information-sharing on the diversion of materiel that could be used to weaponize UAS (e.g. commercial explosives and detonators), including through relevant channels such as INTERPOL Project Watchmaker, the Chemical Anti-Smuggling Enforcement project, the Chemical Risk Identification and Mitigation Project, and the WCO Programme Global Shield.	Establish and maintain a national database of UAS incidents relating to terrorism. Establish and maintain a national database of counter-UAS measures.
3.2. Knowledge sharing	Promote information-sharing between government and non-government sectors on UAS threats and preparedness.	Encourage manufacturers to provide advanced notice to regulators and law enforcement of new UAS and related innovations or product line.	Enhance sharing of information on good practices relating to ways to address the theft, trafficking, diversion, loss and illicit use of materials for weaponizing UAS.	Support research and analysis of the global trends and problems of UAS use by terrorists and other non-State armed groups.

3.2. (*cont'd*)	Regularly convene national and (where appropriate) regional and international stakeholders (i.e. a "community of practitioners") to discuss the technological evolution of UAS, the most effective methods of countering the threat posed by the terrorist use of UAS, and potential gaps in practices and policies, both within and across States. Encourage dialogue and strengthen, where feasible, the exchange of information and good practices with relevant civil society actors, including non-governmental organizations, academia, research institutions and industry.	Provide clear and regularly updated guidance to manufacturers, exporters and distributors regarding the vulnerability of specific multipurpose components to being incorporated for malicious use of UAS.		Consider the sharing of information and lessons-learned (where appropriate) regarding the effectiveness of counter-UAS.
3.3. Awareness-raising	Promote engagement with the public to raise awareness on the safe and compliant use of UAS. Engage with the private sector, industry actors and academia to raise awareness of early-detection measures, precautionary tools and other countermeasures to address threats posed by the terrorist use of UAS. Conduct awareness-raising activities that seek to highlight regulatory requirements and responsibilities for the safe and lawful use of UAS, as well as helping to prepare the public for responses to potential UAS incidents. Encourages States and relevant international and regional organizations and non-governmental organizations (including international industry associations) to continue to build upon existing awareness, prevention and risk education campaigns regarding the urgent threat of weaponized UAS, and to disseminate threat mitigation measures.			
4. Counter-UAS technical measures				
4.1. Threat and vulnerability assessment	Routinely review and consider the probability of, vulnerability to and possible consequences of terrorist uses of UAS.		Monitor and assess new developments relating to the weaponization of UAS, including the availability of materials.	Conduct vulnerability assessments to identify protection gaps, including for critical infrastructure and public targets. Monitor and assess potential threats relating to UAS-specific technological developments and commercial innovations that could facilitate the use of UAS for terrorism purposes.

Table 12 (*continued*)

Policy areas	General	Acquisition	Weaponization	Deployment
4.2. Counter-UAS capability development	Develop, manage and sustain national processes and functional roles required to effectively counter UAS threats from non-State armed groups. Promote clear and coherent systems for the national oversight of through-life management of UAS and critical components. Designate a national authority responsible for conducting assessments and testing, training and evaluation of counter-UAS technologies, including electronic systems, to verify their capability and utility in specifically identified contexts and locations. Regularly assess organizational capabilities to manage counter-UAS. Carefully consider kinetic and non-kinetic countermeasures and account for mitigation of collateral effects. Consider the establishment of a dedicated national research centre to advance counter-UAS-related research and innovation. Introduce counter-UAS capability assessment tools to identify local and national vulnerabilities and areas for development. Prioritize the establishment of technical capabilities to perform adequate, systematic and sustainable testing of effective countermeasures.		Promote training of specialist personnel and teams capable of technical exploitation, including to undertake (biometric and digital) forensics on recovered UAS and components. Continually update risk assessments in the light of emerging technological developments, and ensure, wherever possible, that countermeasures keep up with developments in UAS technology.	Promote training and equipping of personnel and teams capable of safely and securely responding to an incident, including local first responders and authorities. Ensure that training includes the effective and safe use of kinetic and non-kinetic countermeasures. Provide appropriate training, capabilities, information and knowledge management and technology to United Nations peace operations that are required to counter UAS threats, as appropriate. Institutionalize the technical training and capacity-building of national forces and law enforcement in the use of counter-UAS, including to train authorized personnel and teams in operating counter-UAS technologies and equipment to detect and, if necessary, interdict and/or disable UAS. Develop guidance that make it possible for the relevant authorities to detect and promptly differentiate between legitimate, criminal and terrorist use of UAS in a timely manner. Promote the employment of a broad range of UAS detection tools. Consider promoting the integration of manufacturer-level restrictions, such as geofencing.
4.3. UAS incident safety and security, including protection measures	Establish national protection measures against UAS attacks. Ensure the application of relevant UAS safety and security policies and technical standards by industry and private sector actors.		Promote the training of explosive ordnance disposal operators to safely include UAS and components.	Establish and monitor no-fly zones and technical restrictions such as geofencing in relation to critical infrastructure and other sensitive sites.

4.4. Recovery and technical exploitation of UAS and components	Promote specialized training and capacity-building for the technical exploitation of UAS and components, including digital forensic capability. To that end, increase the capacity of law enforcement to recover, analyse and preserve physical, biometric and digital evidence of UAS and UAS components. In aiding investigations, ensure that the chain of custody of the evidence is always maintained, and the integrity of the evidence secured along the process.	Conduct documentation, identification and tracing of recovered UAS and critical components.	Conduct documentation, identification and tracing of recovered material that was used to weaponize UAS.	Consider, consistent with national law, exploitation and analysis of electronic systems associated with aircraft navigation, communications systems and recovered imagery used for terrorism purposes.
4.5. Enforcement measures and criminal justice processes	Establish enforcement measures for those individuals and entities involved in the illicit acquisition, weaponization and deployment of UAS and related components. Evaluate the effectiveness of national criminal justice systems and processes to adequately address terrorist and criminal uses of UAS and components.	Establish specific enforcement measures for those individuals and entities involved in the illicit acquisition of UAS and related components. Apply appropriate penalties – in accordance with national legislation and obligations under international human rights law – against UAS producers, vendors and exporters that do not comply with domestic regulations, or otherwise facilitate violations.	Establish specific enforcement measures for those individuals and entities involved in the weaponization of UAS and related components.	Establish specific enforcement measures for those individuals and entities involved in the deployment of weaponized UAS.
5. Monitoring and diagnostics				
5.1. Monitoring	Establish a national process for conducting end-use or end-user monitoring, including to investigate diverted UAS for use by terrorists.	Develop and implement national processes to monitor and track suspicious purchases and transfers of UAS. Conduct tracing of diverted and recovered UAS and UAS components. Maintain a database of UAS and related components acquired and used by terrorist groups and individuals. Maintain a database of reported lost and stolen UAS and related critical components.	Heighten monitoring for sales of chemical and precursor materials that can be used to weaponize UAS, as appropriate. Monitor and maintain records of the types of UAS weaponization. Identify and maintain records of entities that have weaponized UAS. Monitor so-called “breaker apps” and online guidance in overriding manufacturer controls.	Monitor and maintain records of UAS deployment and uses. Identify and maintain records of entities that have deployed UAS for malicious uses.
5.2. Investigation	Promote domestic efforts – and cooperation between States – on tracing, investigations, prosecutions and judicial proceedings in relation to the diversion and misuse of UAS in the context of counterterrorism.	Take reasonable measures to identify the origin (manufacturer or, in cases of diversion, lawful end user) of recovered UAS for further analysis.	Where consistent with national law, consider the analysis and use of biometric evidence (e.g. DNA and fingerprints) from UAS components recovered after operational use to aid the identification of perpetrators.	Conduct (as part of investigative efforts of UAS incidents) physical, digital and forensic analysis to identify the broader network behind a UAS attack.

Table 12 (*continued*)

Policy areas	General	Acquisition	Weaponization	Deployment
5.2. (*cont'd*)	Make use of all available information to aid investigations, which may include operator licensing, UAS registration information and export control regulations for the identification of perpetrators, as well as electronic remote identification systems to analyse flight patterns. Build specialized capacity of investigators to investigate UAS-related incidents, including knowledge of certain technologies. Promote information-sharing on lessons learned from prosecutions and law enforcement activities.	Investigate diversion of UAS through the analysis of any marks applied to UAS, its critical components or its packaging, and by consulting any existing corresponding transfer and inventory records.	Where consistent with national law, consider analysis of imagery or communications data recovered and extracted from the non-volatile memory in the electronic systems of UAVs, in order to identify those involved in the acquisition, weaponization and operation of UAS.	
5.3. Reporting		Encourage industry to assist States in identifying and reporting suspicious UAS acquisitions that may trigger new law enforcement investigations. Encourage voluntary reporting of seizures of UAS to the WCO Customs Enforcement Network.		Make use of relevant UAS incident reporting templates (e.g. the INTERPOL UAS incident reporting template).
6. Multilateral initiatives, cooperation and assistance				
6.1. Multilateral initiatives and cooperation	Develop an international normative framework to address proliferation and control non-State access to UAS. Strengthen and reaffirm a global norm against technical and material support to non-State groups and to deter and stigmatize entities responsible for the proliferation of UAS capabilities. Consider the development of key terms and concepts for counter-UAS at the global level. Use, promote and enhance relevant international and regional standards, guidelines and good practices on the safe and secure use of UAS, including the "Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017)". Recognize and (where appropriate) support new and existing regional or subregional mechan sms that address UAS threats posed by non-State armed groups. Consider initiating consultative exchanges with industry and technology experts, including under the auspices of the United Nations, and where appropriate, to explore current and emerging threats and solutions against the terrorist use of UAS.			
6.2. Assistance facilitation, including technical, legal, financial support	Encourage States, the United Nations and international, regional and other organizations with relevant expertise to render to interested States – upon their request – technical, financial and material assistance aimed at strengthening the capacity of such States to counter the threat of UAS. This could include assistance in developing good practices for the protection of civilians and infrastructure from attacks, developing standards to ensure the safety of personnel involved in responding to UAS incidents safely and securely, and to provide appropriate assistance to the victims of such attacks. Consider integrating into mandates of United Nations missions a provision on capacity-building assistance for national stakeholders, to counter the threat of non-State use of UAS in situations where such a threat is deemed to be high. Consider the establishment of a common funding pool to provide technical counter-UAS capacity-development assistance to low-capacity and affected States.			

Annex: online questionnaire

Assessing trends in acquisition, weaponization and deployment of unmanned aircraft systems (UAS) by non-State armed groups for terrorism-related purposes

Access link: conflictarm.org/UAS_Questionnaire

The following questionnaire has been edited lightly; for example, the term "non-State actors" has been changed to "non-State armed groups", because the terminology has since become obsolete. The original questionnaire can be consulted via the access link.

1. EMAIL

Email	

2. PROJECT BACKGROUND

The proliferation and acquisition of unmanned aircraft systems (UAS) and related components by non-State armed groups poses a threat to international peace and security. In recent years, the proliferation of UAS software, hardware, and components as well as their weaponization and use by terrorist groups and other criminal actors has increased sharply. According to recent research conducted by the United Nations (UN), by 2020 at least 20 armed non-State armed groups, including terrorist groups, had reportedly obtained, or acquired UAS and related components.

Currently, the United Nations Office of Counter-Terrorism (UNOCT) Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS) and Conflict Armament Research (CAR) are producing a global report on the acquisition, weaponization, and deployment of UAS by illicit non-State armed groups.

This questionnaire was developed by UNOCT and CAR to gather information on Member State experiences, concerns, and priorities regarding UAS-related terrorist threats.

In this questionnaire, "State" is used to refer to your Member State (country).

3. ACKNOWLEDGEMENT OF SURVEY PARTICIPATION

Unless indicated below, the final study will acknowledge your State's participation in this survey by the State's name. If the responding State does not wish to be acknowledged in the final study for participating in this survey, please check the box below:

☐ DO NOT acknowledge my State's participation in this survey in the final study.

4. RESPONDENT DETAIL

The respondent detail information entered below will be protected and treated with full confidentiality.

Completed by (name):	
Title/position/rank:	
Date and Location (state and/or city):	

5. MEMBER STATE DETAIL

Member State (name of your country)	
Entity (ministry, department, unit, etc.)	

Unless indicated below, the survey respondent named above authorizes that all information provided in this survey, including the country name and ministry/agency, may be used in the final report of this study. If you do not wish the following details to be attributed to specific responses in the final report, please check the relevant box(es):

☐ Withhold name of State

☐ Withhold name of ministry/agency

6. PART A: NATIONAL EXPERIENCE OF NON-STATE USE OF UAS

Four (4) questions

Questions to establish a baseline of understanding of Member State's experiences of UAS incidents, including how States record information relating to those incidents.

1. Has your State/entity experienced attacks, disruption, or other incidents involving the use of UAS by malicious, criminal, or terrorist actors?	YES ☐	NO ☐
If YES please provide details of these incidents, including, if possible: accurate or approximate dates, timeframes, UAS types (brand and model or category e.g. micro, mini, commercial, improvised) and actors responsible (specific group if known or suspected category e.g. organized crime, terrorist group, etc).		

2. Does your State/entity maintain national database(s) of UAS incidents and attempted incidents, or otherwise maintain a centralized register of reports of malicious, criminal, or terrorist acts involving UAS? If NO, please proceed to Part B.	YES ☐	NO ☐
If YES please provide details:		

3. If you answered YES to Question 2, which entities are responsible for updating and managing that database or centralizing incident reports?

4. If you answered YES to Question 2, which kinds of information are currently recorded to support your State/entity in understanding and responding to UAS threats?

	YES	NO	Additional information
Actor(s) responsible	☐	☐	
UAS type(s) involved	☐	☐	
Incident target type(s)	☐	☐	
Casualties	☐	☐	
Gender-disaggregated impacts	☐	☐	
Physical damage	☐	☐	
Other	☐	☐	

Please provide any additional information you wish to share on this topic:

7. PART B: UAS ACQUISITION

Seven (7) questions

Questions relating to observed trends in how malicious, criminal, and terrorist actors procure or otherwise gain access to UAS and UAS components, including whether your Member State has recovered UAS in your national territory.

1. In which ways have malicious, criminal, or terrorist actors operating in your State acquired – or attempted to acquire – UAS and UAS components? Please tick all that apply.			
Acquisition type	Materiel type	YES	NO
A. State-sponsored diversion (a process by which a State backs a direct supply of items to unauthorised users)	i. UAS	☐	☐
	ii. UAS components	☐	☐
	iii. UAS technology	☐	☐
B. Commercial off-the-shelf (COTS) (purchase of commercially available products and technology, either legally or illegally)	i. UAS	☐	☐
	ii. UAS components	☐	☐
	iii. UAS technology	☐	☐
C. Illicit manufacture or modification (self-design, development, and construction of UAS or UAS components). This can either refer to the manufacture of an entire system or modifying one already in existence	i. UAS	☐	☐
	ii. UAS components	☐	☐
	iii. UAS technology	☐	☐
D. Illicit trafficking (cross-border movement of materiel including postal shipments)	i. UAS	☐	☐
	ii. UAS components	☐	☐
	iii. UAS technology	☐	☐
E. Loss from military or law enforcement during active use and deployment (acquisition through violent capture from national security forces or from private or national law enforcement, or as a result of loss through abandonment or surrender)	i. UAS	☐	☐
	ii. UAS components	☐	☐
	iii. UAS technology	☐	☐
F. Diversion from legitimate state or private custodians (theft, loss, or violent capture from legal custodians, including manufacturers, private civilian owners, or state holdings)	i. UAS	☐	☐
	ii. UAS components	☐	☐
	iii. UAS technology	☐	☐
G. Other (please specify)			

If you ticked OTHER, please specify the ways in which malicious, criminal, or terrorist actors operating in your State acquired – or attempted to acquire – UAS and UAS components.

2. What types of emerging developments and trends relating to terrorist acquisition of UAS are of the greatest concern to your State/entity?

3. In the last ten years, have national authorities in your State/entity seized, intercepted, captured, or otherwise recovered UAS or UAS components from malicious, criminal, or terrorist actors?	YES ☐	NO ☐
If NO, please proceed to question 4. If YES please provide details of recoveries, including dates or timeframes, quantities, and actors from which material was recovered, where possible and appropriate:		

4. If applicable, which agencies have seized, intercepted, captured, or otherwise recovered UAS and UAS-components in your State/entity? Please tick all that apply.

	YES	NO	Additional information
A. Police and law enforcement	☐	☐	
B. Customs or border security agencies	☐	☐	
C. Armed forces	☐	☐	
D. Privately-owned security entities	☐	☐	
E. Other (please specify)	☐	☐	

If you ticked OTHER, please specify which other entities have seized, intercepted, captured, or otherwise recovered UAS and UAS-components in your State:

5. Does your State/entity take precautionary measures to prevent UAS deployed by, or in the possession of, legitimate custodians – both private and state – from being stolen, captured, or shot down by terrorists and non-State actors?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of measures taken by your State.			

6. Is your State/entity aware of instances where malicious, criminal, or terrorist actors have cooperated to acquire UAS, either within your national borders or externally?	YES ☐	NO ☐
If YES please provide details:		

7. If you answered YES to question 6: In which ways have malicious, criminal, or terrorist actors sought to cooperate in acquiring UAS? Please tick all that apply.			
	YES	NO	Additional information
A. Remote technical advice and support	☐	☐	
B. Procuring UAS technology and plans	☐	☐	
C. Facilitating the procurement and/or transfer of UAS and UAS components	☐	☐	
D. Provision of financing	☐	☐	
E. Other (please specify)	☐	☐	

8. PART C: UAS WEAPONIZATION

Three (3) questions

Questions relating to how Member States observe malicious, criminal, and terrorist actors modifying UAS platforms to increase their threat and lethality.

1. Does your State have legislation to prohibit the modification of commercial or recreational UAS?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of the modifications that are prohibited in your State.			

2. In which of the following ways has your State identified and prevented attempted or actual weaponization of commercial UAS and components in your State, if any? Please tick all that apply.

	YES	NO	Additional information
A. Camera payload	☐	☐	
B. Improvised explosive devices (IEDs)	☐	☐	
C. Conventional munitions	☐	☐	
D. Dispersal or spraying mechanisms	☐	☐	
E. Addition of a release mechanism	☐	☐	
F. Other (please specify)	☐	☐	

If you ticked OTHER, please specify any other ways in which your State/entity identified and prevented attempted or actual weaponization of commercial UAS and components in your State:

Please provide any additional information you wish to share on this topic:

3. What types of emerging technological developments relating to UAS weaponization are of the greatest concern to your State?

9. PART D: UAS DEPLOYMENT

Ten (10) questions

Questions relating to how malicious, criminal, and terrorist actors have sought to use UAS in your State, including information on intended targets. This section also includes questions to establish how Member States regulate civilian and commercial users of UAS as a prevention measure.

1. Have UAS been used, or attempted to be used, for any of the following purposes in your State by malicious, criminal, or terrorist actors? Please tick all that apply.			
	YES	NO	Additional information
A. ISTAR (intelligence, surveillance, target acquisition, reconnaissance)	☐	☐	
B. Targeting support	☐	☐	
C. Direct attack (i.e., suicide drones)	☐	☐	
D. Indirect attack	☐	☐	
E. Swarm attack	☐	☐	
F. Targeted killings	☐	☐	
G. Disruption and interference of key infrastructure, including air traffic and facilities	☐	☐	
H. Collecting footage for use in propaganda	☐	☐	
I. Inciting panic in mass gatherings	☐	☐	
J. Distraction or disruption of law enforcement efforts	☐	☐	
K. Illicit transfers and smuggling of illicit goods	☐	☐	
L. Other (please describe)	☐	☐	

If you ticked OTHER, please specify how UAS have been used, or attempted to be used, for any of the following purposes in your State by malicious, criminal, or terrorist actors:

Please provide any additional information you wish to share on this topic:

2. Have there been actual or attempted incidents of UAS use against any of the following targets in your State? Please tick all that apply.			
	YES	NO	Additional information
A. Airports	☐	☐	
B. Other transport infrastructure (e.g., roads, railways, stations, etc.)	☐	☐	
C. Energy infrastructure and utilities (e.g., power stations, network grids, dams, etc.)	☐	☐	
D. Civilian individuals or groups	☐	☐	
E. Populated areas and public spaces (e.g., markets, stadiums, religious or cultural sites)	☐	☐	
F. Prisons	☐	☐	
G. Law enforcement	☐	☐	
H. First responders	☐	☐	
I. Government buildings	☐	☐	
J. Military personnel	☐	☐	
K. Military buildings or infrastructure	☐	☐	
L. Other non-State actors	☐	☐	
M. Other (please describe)	☐	☐	

If you ticked OTHER, please specify where actual or attempted incidents of UAS use in your State have occurred:

Please provide any additional information you wish to share on this topic:

3. How would you categorize the malicious, criminal, or terrorist actors using, or seeking to use, UAS in your State? Please tick all that apply.			
	YES	NO	Additional information
A. Unaffiliated individuals	☐	☐	
B. Terrorist organizations	☐	☐	
C. Organised crime groups	☐	☐	
D. Other groups (e.g., activists)	☐	☐	
E. Other (please describe)	☐	☐	

If you ticked OTHER, please specify where actual or attempted incidents of UAS use in your State have occurred:

Please provide any additional information you wish to share on this topic:

4. How would you categorize the gender identity and age of non-State actor types using, or seeking to use, UAS in your State? Please select all that apply as well as indicate percentages if possible.			
	YES	NO	Additional information
A. Male	☐	☐	
B. Female	☐	☐	
C. Other	☐	☐	
D. Youth	☐	☐	

Please provide any additional information you wish to share on this topic:

5. Is it legal for private commercial or civilian actors to possess UAS in your State?	YES ☐	NO ☐	With exceptions ☐
If NO (including WITH EXCEPTIONS), please provide details of UAS types that are prohibited for civilian possession in your State.			

6. Does your State/entity require UAS operators (whether individual civilian users or private commercial actors) to have a license to own and use UAS?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details:			

7. Does your State/entity impose any other restrictions or conditions on civilian or commercial use of UAS in your State - for example, requirements relating to storage and safeguarding of UAS, or restrictions on retransfer of UAS?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details:			

8. Does your State/entity impose limits on the types of UAS that civilians can possess (e.g., weight, range, capabilities?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of the limits imposed by your State.			

9. Does your State have “no-drone zones” preventing deployment in specific locations?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please specify which areas are protected from drone overflying in your State.			

10. What types of emerging technological developments relating to UAS deployment are of the greatest concern to your State/entity?

10. Counter-UAS policies and controls

Ten (10) questions

Questions to establish a baseline of measures and policies in each Member State regarding UAS, including whether there is a national focal point for counter-UAS national strategies, and what counter-UAS measures are currently in place.

1. Please describe the primary legislation or regulatory frameworks that apply to the transfer, possession, and use of UAS in your State by civilian, commercial, and state actors.

2. Are UAS or UAS-components manufactured by companies in your State? If NO, please proceed to question 5.	YES ☐	NO ☐

3. If you answered YES to question 2: Does your State have a system in place for licensing the commercial manufacture of UAS or UAS components? If NO, please proceed to question 5.	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of measures taken by your State.			

4. If you answered YES (including WITH EXCEPTIONS) to question 3, does this system include safeguards to prevent or restrict the use of UAS manufactured in your State from being used for terrorist-related purposes? (e.g., inclusion of geo-fencing configurations or electronic remote identification).	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of measures taken by your State.			

5. Does your State require commercial retailers of UAS to keep records of sales of UAS by serial number?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of the information types required by your State.			

6. Does your State/entity cooperate with the private sector to raise awareness with vendors of commercial UAS to help them identify and report suspicious transactions?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details.			

7. Does your State have a national policy or strategy for countering UAS threats, including public awareness activities and training on UAS-related threats and risks?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of the national policy or strategy.			

8. Has your State designated a national counter-UAS coordinating lead entity?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of this lead entity.			

9. Does your State have an official list that categorizes and defines UAS and UAS-components, as well as terminology?	YES ☐	NO ☐	With exceptions ☐
If YES (including WITH EXCEPTIONS), please provide details of this list, and a link if public.			

10. Please list any international cooperation and information sharing mechanisms on UAS in which your State/entity participates.

11. Counter-UAS exploitation and UAS digital forensics

Five (5) questions

Questions relating to Member States' capacity to recover UAS and conduct effective forensic analysis.

1. Does your State/entity have procedures for the recovery and preservation of the following information after a UAS incident?			
	YES	NO	Additional information
A. Physical evidence of UAS and components?	☐	☐	
B. Biometric evidence of UAS and components	☐	☐	
C. Digital evidence of UAS and components?	☐	☐	

2. Are there examples of successful prosecutions in your State of individuals who have unlawfully acquired, weaponized, or deployed UAS for use in criminal or terrorist incidents?	YES ☐	NO ☐
If **YES**, please provide relevant examples if appropriate to do so.		

3. Do the national authorities in your State have the capacity to convene a complete digital forensics procedure with a captured or countered UAS?	YES ☐	NO ☐
If **YES**, please write down which compendium, manual or other material you have to complete such a digital forensics procedure:		

4. Have the national authorities in your State ever presented UAS digital forensics in court?	YES ☐	NO ☐
If **YES**, please provide details of the case(s) as appropriate:		

5. Do the national authorities in your State have appropriate facilities (laboratory or similar) to convene a UAS digital forensics procedure with a seized, intercepted, captured, or otherwise recovered UAS?	YES ☐	NO ☐
If **NO**, please write down if building such facilities is planned or otherwise something of interest:		

Please provide any additional information, or elaborate on any other relevant UAS countermeasures and controls that your State applies, as appropriate:

12. Programme specific feedback

1. Please indicate what types of assistance, if any, you believe your State/entity would benefit from to counter the acquisition, weaponization, and deployment of UAS by non-State actors for terrorism-related purposes:

2. Please indicate what type of capacity-building you believe UNOCT's Global AROS Programme should prioritize when assisting Member States to counter the acquisition, weaponization, and deployment of UAS by non-State actors for terrorism-related purposes:

3. UNOCT's Global AROS Programme is well positioned to gather the international community for awareness-raising and the sharing of information and good practices. What topics, if any, relating to countering the acquisition, weaponization, and deployment of UAS by non-State actors for terrorism-related purposes, would you like to see discussed?

Bibliography

Almohammad, Assad, and Anne Speckhard (2017). ISIS drones: evolution, leadership, bases, operations and logistics. International Center for the Study of Violent Extremism. 5 May. Available at https://icsve.org/isis-drones-evolution-leadership-bases-operations-and-logistics.

Al-Haj, Ahmed (2022). Yemeni rebel drones target Greek ship in government-run port. *Associated Press*, 22 October. Available at https://apnews.com/article/iran-houthis-middle-east-sanaa-yemen-04ce841d3268f200e393bf7d71e767e3.

Batrawy, Aya (2022). Drone attack in Abu Dhabi claimed by Yemen's rebels kills 3. *Associated Press*, 17 January. Available at https://apnews.com/article/business-dubai-united-arab-emirates-abu-dhabi-yemen-8bdefdf900ce46a6fd6c7bc685bf838a.

BBC News (2015). Japan radioactive drone: Tokyo police arrest man. 25 April. Available at www.bbc.co.uk/news/world-asia-32465624.

_____ (2021). Mexico cartel used explosive drones to attack police. 21 April. Available at www.bbc.co.uk/news/world-latin-america-56814501.

Borrie, John, Elena Finckh and Kerstin Vignard (2017). *Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles*. Geneva: United Nations Institute for Disarmament Research. Available at https://unidir.org/publication/increasing-transparency-oversight-and-accountability-armed-unmanned-aerial-vehicles.

CAR (Conflict Armament Research) (2016a). Tracing the supply of components used in Islamic State IEDs. Available at www.conflictarm.com/reports/tracing-the-supply-of-components-used-in-islamic-state-ieds.

_____ (2016b). Islamic State's weaponised drones. Available at www.conflictarm.com/perspectives/islamic-states-weaponised-drones.

_____ (2017a). Iranian technology transfers to Yemen. Available at www.conflictarm.com/perspectives/iranian-technology-transfers-to-yemen.

_____ (2017b). Islamic State's multi-role IEDs. Available at www.conflictarm.com/perspectives/multi-role-ieds.

_____ (2018). Conventional ammunition diversion. Available at www.conflictarm.com/technical/conventional-ammunition-diversion.

_____ (2020a). Evolution of UAVs employed by Houthi forces in Yemen. Available at www.conflictarm.com/dispatches/evolution-of-uavs-employed-by-houthi-forces-in-yemen.

_____ (2020b). Procurement networks behind Islamic State improvised weapon programmes. Available at www.conflictarm.com/reports/procurement-networks-behind-islamic-state-improvised-weapon-programmes.

_____ (2021). Weapons of the war in Ukraine. Available at www.conflictarm.com/reports/weapons-of-the-war-in-ukraine.

Chávez, Kerry, and Ori Swed (2020). Off the shelf: the violent nonstate actor drone threat. *Air & Space Power Journal* (Fall). Available at www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf.

_____ (2021). The proliferation of drones to violent nonstate actors. *Defence Studies*, vol. 21, No. 1, pp. 1–24.

_____ (2023a). The drivers of drone innovation by violent nonstate actors (DDIV) dataset. Working Paper.

_____ (2023b). The empirical determinants of violent nonstate actor drone adoption. *Armed Forces & Society*.

CTC (Counter-Terrorism Committee) (2022). Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes. Available at www.un.org/securitycouncil/ctc/news/delhi-declaration-countering-use-new-and-emerging-technologies-terrorist-purposes-now-available.

Dass, Reuben (2022). Militants and drones: a trend that is here to stay. Royal United Services Institute. 6 September. Available at www.rusi.org/explore-our-research/publications/commentary/militants-and-drones-trend-here-stay.

DroneSec (2023). Stolen Drones Info. Available at https://stolendrone.info/home.

Ekelhof, Merel, and Giacomo Persi Paoli (2020). *Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems*. Geneva: United Nations Institute for Disarmament Research. Available at www.unidir.org/sites/default/files/2020-04/UNIDIR%20Swarm%20Robotics%20-%202020.pdf.

European Union Aviation Safety Agency (2021). *Drone Incident Management at Aerodromes – Part 1: the Challenge of Unauthorised Drones in the Surroundings of Aerodromes*. Cologne, Germany. Available at www.easa.europa.eu/sites/default/files/dfu/drone_incident_management_at_aerodromes_part1_website_suitable.pdf.

Fernando, Lorenz Anthony T. (2022). Armed unmanned aerial vehicles: the need for stronger export controls. Asia-Pacific Leadership Network. 4 April. Available at www.apln.network/analysis/commentaries/armed-unmanned-aerial-vehicles-the-need-for-stronger-export-controls.

Gettinger, Dan (2023). One-way attack drones: loitering munitions of past and present. Vertical Flight Society. 4 May.

Gibbons-Neff, Thomas (2016). ISIS used an armed drone to kill two Kurdish fighters and wound French troops, report says. *The Washington Post*, 11 October. Available at www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says.

Global Counterterrorism Forum (2019). Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems. Available at www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fI%3D&portalid=1.

Grand-Clément, Sarah, and Theò Bajon (2022a). *Uncrewed Aerial Systems: A Primer*. Geneva: United Nations Institute for Disarmament Research. Available at https://unidir.org/publication/uncrewed-aerial-systems-primer.

_____ (2022b). *Uncrewed Ground Systems: A Primer*. Geneva: United Nations Institute for Disarmament Research. Available at www.unidir.org/sites/default/files/2022-11/UNIDIR_Uncrewed_Ground_Systems_Primer.pdf.

Haider, Lieutenant Colonel André (2021). Unmanned aircraft system threat vectors. In *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Kalkar, Germany: Joint Air Power Competence Centre, pp. 33–52. Available at www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems.

Hambling, David (2021). Mexican cartel injures police officers with drone bomb attack (update: second cartel allegedly using weaponized drones). *Forbes*, 22 April. Available at www.forbes.com/sites/davidhambling/2021/04/22/mexican-cartel-injures-police-officers-with-drone-bomb-attack/?sh=2bf2aeb0127a.

Haugstvedt, Håvard (2021). A flying threat coming to Sahel and East Africa? A brief review. *Journal of Strategic Security*, vol. 14, No. 1. Available at https://doi.org/10.5038/1944-0472.14.1.1848.

Hoenig, Milton (2014). Hezbollah and the use of drones as a weapon of terrorism. Federation of American Scientists. 5 June. Available at https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism.

Holland Michel, Arthur (2020). Unarmed and dangerous: the lethal applications of non-weaponized drones. Center for the Study of the Drone at Bard College. Available at https://dronecenter.bard.edu/files/2020/03/CSD-Unarmed-and-Dangerous-Web.pdf.

ICAO (International Civil Aviation Organization) (n.d. a). The ICAO UAS Toolkit. Available at www.icao.int/safety/UA/UASToolkit/Pages/default.aspx.

_____ (n.d. b). Introduction to ICAO Model UAS Regulations. Available at www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx.

_____ (2011). *Unmanned Aircraft Systems (UAS).* ICAO Cir 328. Montréal, Quebec, Canada. Available at www.icao.int/meetings/uas/documents/circular%20328_en.pdf.

_____ (2020). Protection of civil aviation infrastructure against unmanned aircraft. Restricted.

International Crisis Group (2018). Saving Idlib from destruction. 3 September. Available at www.crisisgroup.org/middle-east-north-africa/eastern-mediterranean/syria/b63-saving-idlib-destruction.

INTERPOL (International Criminal Police Organization) and Norwegian Police (2022). INTERPOL drone countermeasure exercise report. Available at www.interpol.int/content/download/17737/file/CUAS_Interpol_Low_Final.pdf.

Inter-Agency Working Group on Disarmament, Demobilization and Reintegration (2006). 1.20 Glossary: terms and definitions. In *Integrated Disarmament, Demobilization and Reintegration Standards.* New York: United Nations. Available at www.unddr.org/modules/IDDRS-1.20-Glossary.pdf.

Jalal, Ibrahim (2023). Under pressure: Houthis target Yemeni government with economic warfare. Middle East Institute. 27 February. Available at www.mei.edu/publications/under-pressure-houthis-target-yemeni-government-economic-warfare.

Kallenborn, Zachary (2022). InfoSwarms: drone swarms and information warfare. *Parameters*, vol. 52, No. 2. Available at https://press.armywarcollege.edu/parameters/vol52/iss2/13.

Kallenborn, Zachary, Gary Ackerman and Philipp C. Bleek (2022). A plague of locusts? A preliminary assessment of the threat of multi-drone terrorism. *Terrorism and Political Violence*, vol. 35, No. 7. Available at www.tandfonline.com/doi/abs/10.1080/09546553.2022.2061960.

MacKenzie, Lieutenant Colonel Paul, and Major Fotios Kanellos (2021). Cyberspace operations. In *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Kalkar, Germany: Joint Air Power Competence Centre, pp. 183–207. Available at www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems.

Malaret Baldo, Alfredo, Manuel Martinez Miralles, Erica Mumford and Natalie Briggs (2021). The Arms Trade Treaty: Diversion Analysis Framework. United Nations Institute for Disarmament Research, Conflict Armament Research and Stimson Center. ATT Issue Brief No. 3. Available at www.unidir.org/sites/default/files/2021-08/ATT_Issue_Brief_3-Diversion_Analysis_Framework.pdf.

Martin, Brad, and others (2013). *Assessment of Joint Improvised Explosive Device Defeat Organization (JIEDDO) Training Activity*. RAND Corporation. Available at www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR421/RAND_RR421.pdf.

Muhsin, Dhia (2019). Houthi use of drones delivers potent message in Yemen War. International Institute for Strategic Studies. 27 August. Available at www.iiss.org/online-analysis/online-analysis//2019/08/houthi-uav-strategy-in-yemen.

Paton Walsh, Nick, and others (2019). Inside the August plot to kill Maduro with drones. CNN. 21 June. Available at https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html.

Rassler, Don (2016). *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology.* West Point, New York: Combating Terrorism Center, United States Military Academy. Available at https://ctc.westpoint.edu/wp-content/uploads/2016/10/Drones-Report.pdf.

_____ (2018). *The Islamic State and Drones: Supply, Scale, and Future Threats*. West Point, New York: Combating Terrorism Center, United States Military Academy. Available at https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf.

Reid, David (2018). A swarm of armed drones attacked a Russian military base in Syria. CNBC. 11 January. Available at www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html.

Reuters (2016). Islamic State drone kills two Kurdish fighters, wounds two French soldiers. 11 October. Available at www.reuters.com/article/us-france-iraq-iraq-idUSKCN12B2QI.

Rogers, James (2019). The dark side of our drone future. Bulletin of the Atomic Scientists. 4 October. Available at https://thebulletin.org/2019/10/the-dark-side-of-our-drone-future.

_____ (2022). Address to the United Nations Security Council Arria-formula meeting on “Threats to international peace and security caused by transnational activities of terrorist groups”. Available at https://media.un.org/en/asset/k1q/k1qcqls4b9.

_____ (2023). The second drone age: defining war in the 2020s. *Defense & Security Analysis*, vol. 39, No. 2.

Rogers, James, and Dominika Kunertova (2022). The vulnerabilities of the drone age: established threats and emerging issues out to 2035 – final report. Center for War Studies and Center for Security Studies. Available at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/NATO_VDA_Policy_Report.pdf.

Schori Liang, Christina (2023). Terrorist digitalis: preventing terrorists from using emerging technologies. In *Global Terrorism Index 2023*. Sydney: Institute for Economics & Peace. pp. 72–74. Available at www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf.

Seddon, Bob, and Alfredo Malaret Baldo (2020). Counter-IED capability maturity model & self-assessment tool. United Nations Institute for Disarmament Research. Available at https://unidir.org/sites/default/files/2020-06/Final%20-%20UNIDIR%20Counter-IED%20Self%20Assessment%20Tool.pdf.

United Kingdom, Ministry of Defence (2017). *Joint Doctrine Publication 0-30.2. Unmanned Aircraft Systems.* Swindon: Development, Concepts and Doctrine Centre. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf.

United Nations, General Assembly (2020). Use of armed drones for targeted killings: report of the Special Rapporteur on extrajudicial, summary or arbitrary executions. 15 August. A/HRC/44/38.

_____ (2021). The United Nations Global Counter-Terrorism Strategy: seventh review. 2 July. A/RES/75/291.

_____ (2023). The United Nations Global Counter-Terrorism Strategy: eighth review. 3 July. A/RES/77/298.

United Nations, Security Council (2018). Final report of the Panel of Experts on Yemen. 26 January. S/2018/68.

_____ (2019). Final report of the Panel of Experts on Yemen. 25 January. S/2019/83.

_____ (2021). Final report of the Group of Experts on the Democratic Republic of the Congo. 10 June. S/2021/560.

_____ (2022a). Final report of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140 (2014). 26 January. S/2022/50.

_____ (2022b). Letter dated 11 July 2022 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council. 15 July. S/2022/547.

_____ (2022c). Statement by the President of the Security Council. 9221st meeting on "Threats to international peace and security caused by terrorist acts". 15 December. S/PRST/2022/7.

_____ (2023a). Final report of the Group of Experts on the Democratic Republic of the Congo. 13 June. S/2023/431.

_____ (2023b). Letter dated 13 February 2023 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council. 13 February. S/2023/95.

_____ (2023c). Letter dated 24 July 2023 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council. 25 July. S/2023/549.

_____ (2023d). Fourteenth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2665 (2022) concerning the Taliban and other associated individuals and entities constituting a threat to the peace stability and security of Afghanistan. 1 June. S/2023/370.

United Nations Office of Counter-Terrorism (UNOCT) (n.d.). Launch of the United Nations network of experts on the protection of vulnerable targets against terrorist attacks. Available at www.un.org/counterterrorism/events/launch-united-nations-network-experts-protection-vulnerable-targets-against-terrorist-attacks.

University of Maryland (n.d.). Global Terrorism Database. Available at www.start.umd.edu/gtd.

UNOCT United Nations Counter-Terrorism Centre and the United Nations Interregional Crime and Justice Research Institute (UNICRI) (2021a). *Science, Technology and Innovation: Understanding Advancements from the Perspective of Countering Weapons of Mass Destruction Terrorism*.

_____ (2021b). *Algorithms and Terrorism: the Malicious Use of Artificial Intelligence for Terrorist Purposes.* New York: UNOCT. Available at www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

UNOCT United Nations Counter-Terrorism Centre, Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Institute for Disarmament Research, and the United Nations Global Counter-Terrorism Coordination Compact (2022). Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons. Available at www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/technical_guidelines_to_facilitate_the_implementation_of_security_council_resolution_2370_2017_and_related_international_standards_and_good_practices_on_preventing_terrorists_from_acquiring_weapons.pdf.

UNOCT, CTED and INTERPOL (2022). The protection of critical infrastructure against terrorist attacks: compendium of good practices, 2022 update. Available at www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf.

UNOCT, CTED, the United Nations Alliance of Civilizations (UNAOC) and UNICRI (2022). Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS): Good practices guide – specialized module 5. Available at www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf.

UN News (2017). Feature: Does drone technology hold promise for the UN? 6 September. Available at https://news.un.org/en/story/2017/09/564452-feature-does-drone-technology-hold-promise-un.

US Customs and Border Protection (2023). Human smugglers now using drones to surveil USBP. Media Releases. 1 March. Available at www.cbp.gov/newsroom/local-media-release/human-smugglers-now-using-drones-surveil-usbp.

US Department of the Treasury (2015). Treasury sanctions Hizballah procurement agents and their companies. Press Releases. 5 November. Available at https://home.treasury.gov/news/press-releases/jl0255.

Veilleux-Lepage, Yannick, and Emil Archambault (2022). *A Comparative Study of Non-State Violent Drone Use in the Middle East*. The Hague: International Centre for Counter-Terrorism. Available at www.icct.nl/publication/comparative-study-non-state-violent-drone-use-middle-east.

Verbruggen, Maaike (2019). The question of swarms control: challenges to ensuring human control over military swarms. EU Non-proliferation and Disarmament Consortium. No. 65, December. Available at www.nonproliferation.eu/wp-content/uploads/2019/12/EUNPDC_no-65_031219.pdf.

Waters, Nick (2019). Houthis use armed drone to target Yemeni army top brass. *Bellingcat*, 10 January. Available at www.bellingcat.com/news/mena/2019/01/10/houthis-use-armed-drone-to-target-yemeni-army-top-brass.

Watts, Tom, and Ingvild Bode (2023). Automation and Autonomy in Loitering Munitions Catalogue (v.1). Zenodo. Available at https://zenodo.org/records/7860762.

Weiss, Caleb (2018). Al Qaeda group JNIM releases high-level production video. *FDD's Long War Journal*, 21 March. Available at www.longwarjournal.org/archives/2018/03/al-qaeda-group-jnim-releases-high-level-production-video.php.

Zhang, Min, and Tom Daly (2019). Commercial pig farm in China jams drone signal to combat swine fever crooks. *Reuters*, 20 December. Available at www.reuters.com/article/china-swinefever-idUSL4N28U0QB.

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

Autonomous and Remotely Operated Systems

AROS PROGRAMME

bit.ly/OCT-AROS